(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Offenlegungsschrift**

(10) **DE 101 26 752 A 1**

(51) Int. Cl.[7]: G 06 F 17/30

(21) Aktenzeichen: 101 26 752.5
(22) Anmeldetag: 1. 6. 2001
(43) Offenlegungstag: 20. 12. 2001

DE 101 26 752 A 1

(30) Unionspriorität:
594882 15. 06. 2000 US

(71) Anmelder:
International Business Machines Corp., Armonk, N.Y., US

(74) Vertreter:
Gigerich, J., Dipl.-Ing., Pat.-Ass., 70563 Stuttgart

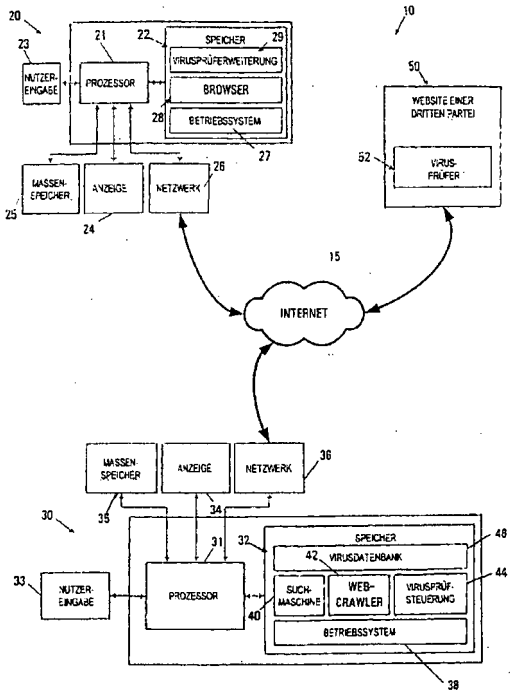
(72) Erfinder:
Bates, Cary Lee, Rochester, Minn., US; Crenshaw, Robert James, Apex, N.C., US; Day, Paul Reuben, Rochester, Minn., US; Santosuosso, John Matthew, Rochester, Minn., US

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) Virusprüfung und -meldung für Suchergebnisse von Computerdatenbanken

(57) Ein System, ein Programmprodukt und ein Verfahren integrieren Virusprüffunktionalität in eine Suchumgebung einer Computerdatenbank, um beim Schutz eines Nutzercomputers vor dem Einfangen eines Computervirus zu assistieren, wenn auf Suchergebnisse zugegriffen wird. Die Erzeugung einer Anzeigedarstellung einer Ergebnismenge, die als Antwort auf eine Suchanfrage erzeugt wird, kann wenigstens zum Teil auf Informationen zum Virusstatus basieren, die wenigstens einem Teil einer Vielzahl von Ergebnisdatensätzen zugeordnet sind, die in der erzeugten Ergebnismenge identifiziert wurden. Darüber hinaus konfigurieren ein System, ein Programmprodukt und ein Verfahren einen ersten Computer, um Informationen zum Virusstatus, die von einer Vielzahl von Computern erzeugt wurden, zu empfangen, wobei die derart empfangenen Informationen zum Virusstatus in einer Virusdatenbank gespeichert werden, die für den ersten Computer zugänglich ist.



DE 101 26 752 A 1

Beschreibung

Bereich der Erfindung

[0001] Die Erfindung bezieht sich allgemein auf Computer und Computersoftware. Spezieller bezieht sich die Erfindung auf die Virenprüfung und das Suchen (scannen) nach Viren sowie das Durchsuchen von Computerdatenbanken.

Hintergrund der Erfindung

[0002] Die Menge und die Vielzahl von Informationen, auf die durch einen Computer zugegriffen werden kann, wächst weiter mit einer erstaunlichen Geschwindigkeit. Insbesondere das Internet hat Computernutzer in die Lage versetzt, auf eine große Vielzahl von Informationen auf anderen Computern, die sich überall auf der Welt befinden, zuzugreifen.

[0003] In dem Maße wie Computer mehr und mehr verschiedenen Informationsquellen zugeordnet sind, unterliegen sie jedoch steigend dem Risiko, Computerviren einzufangen. Ein Computervirus kann im Allgemeinen jedes bösartige oder anderweitig verdeckte Computerprogramm umfassen, das einen Computer "infiziert" und unerwünschte Aktivitäten im Computer ausführt. Einige Computerviren sind ihrer Natur nach einfach nur eine Dummheit, andere Viren können jedoch eine beträchtliche Menge Schaden an einem Computer und/oder seinem Nutzer anrichten, bis hin zum Stehlen privater Daten, zum Löschen von Daten und/oder zum Verursachen eines kompletten Computerausfalls. Einige Viren erlauben sogar einer dritten Partei, die Steuerung eines Computers des Nutzers außerhalb des Wissens des Nutzers zu erlangen, während andere einen Computer des Nutzers benutzen können, um andere bösartige Aktivitäten, zum Beispiel das Starten von Angriffen der Art "Verweigerung des Dienstes" (DOS) gegen andere Computer, auszuführen.

[0004] Viren können viele verschiedene Formen annehmen und in einer Vielzahl von Arten verbreitet werden, zum Beispiel als E-Mail-Anlagen, als Makros oder Scripts, als Trojanische Pferde, Würmer, Logikbomben usw. (auf alle wird für die jetzigen Zwecke als "Viren" Bezug genommen). Ein Virus wird sich oft verstecken oder ein ansonsten gesundes Computerprogramm "infizieren", so dass der Virus aktiviert wird, wenn das infizierte Computerprogramm ausgeführt wird. Viren haben typischerweise auch die Fähigkeit, sich zu vermehren und sich auf andere Computerprogramme und auch auf andere Computer zu übertragen.

[0005] Um auf die mit Viren verbundenen Risiken einzugehen, wurden beträchtliche Anstrengungen auf die Entwicklung von Anti-Virus-Computerprogrammen gerichtet, die versuchen, Viren, die einen Computer infizieren wollen, zu erkennen und/oder zu entfernen. Solche Versuche resultierten in einem ständigen Wettbewerb, in dem Virenentwickler ständig versuchen, immer höher entwickelte Viren zu schaffen, und Anti-Virus-Entwickler ständig versuchen, Computer vor neuen Viren zu schützen.

[0006] Eine Fähigkeit von vielen konventionellen Anti-Virusprogrammen ist die Fähigkeit, die Virenprüfung von virusverdächtigen Computerdateien auszuführen, nachdem diese Dateien empfangen und auf einem Computer gespeichert wurden, zum Beispiel nach dem Herunterladen von Emails oder ausführbaren Dateien vom Internet. Serverbasierte Anti-Virusprogramme werden auch typischerweise genutzt, um die für einen Server zugänglichen Dateien auf Viren zu überprüfen. Solche Anti-Virusprogramme werden zum Beispiel oft von Websites aus internen Gründen genutzt, speziell von Sites zum Herunterladen, die Nutzerzugang zu einer großen Zahl von herunterladbaren, ausführbaren Dateien gewähren, die relativ oft virusverdächtig sind.

[0007] Das Virusprüfen ist oft sowohl prozessor- als auch bandbreitenintensiv, und infolgedessen sind konventionelle Anti-Virusprogramme typischerweise auf die Ausführung von Virusprüfungen für Dateien beschränkt, die im Allgemeinen auf den gleichen Computern gespeichert sind, auf denen solche Programme ausgeführt werden. Während daher bestimmte Entitäten, inklusive Endnutzer und Websites, Virusprüfungen mit Dateien, die lokal auf Computern dieser Entitäten gespeichert sind, ausführen können, sind diese Entitäten oftmals nicht fähig, die viralen Risiken zu bestimmen, die Dateien unter der Steuerung von anderen Entitäten zugeordnet sind, wenigstens nicht, bis solche Dateien beschafft und lokal von einem Anti-Virusprogramm geprüft werden können.

[0008] Insbesondere die verteilte und dezentralisierte Natur des Internets und anderer gemeinsam benutzter Computernetzwerke hebt die obengenannten Beschränkungen der konventionellen Anti-Virustechnologien hervor, da ein Nutzer oftmals durch eine große Vielzahl von Websites steuert und fähig ist, virusverdächtige Dateien von einer großen Zahl von Entitäten außerhalb der Steuerung des Nutzers herunterzuladen.

[0009] Ein besonderes Beispiel für die Risiken ist das Ausführen von internetbasiertem Suchen und der Zugriff auf die hierbei erstellten Suchergebnisse. Höherentwickelte Suchmaschinen und zugeordnete "Portal"-Sites wurden von Suchprovidern mit dem besonderen Ziel entwickelt, Nutzern die Lokalisierung von Websites, Webseiten und anderen für Nutzer interessanten Dateien zu erleichtern. Viele konventionelle Suchmaschinen unterhalten zum Beispiel index- und/oder verzeichnisbasierte Computerdatenbanken, die versuchen, Inhalte im Internet aufzulisten, so dass relevante Webseiten oder andere Dateien von Nutzern als Antwort auf Suchanfragen, die von diesen Nutzern an die Suchmaschinen geschickt werden, erkannt werden können. Oft umfassen solche Datenbanken eine große Zahl von Datensätzen, die verschiedenen Dateien zugeordnet sind, so dass eher die Datensätze selbst als die Dateien durchsucht werden.

[0010] Suchergebnisse werden typischerweise an einen Nutzer der Suchmaschine in Form einer formatierten Liste von Einträgen oder Datensätzen zurückgegeben, die Dateien zugeordnet sind, zum Beispiel Webseiten, die der Anfrage entsprechen. Oft werden Hypertextlinks bereitgestellt, so dass ein Nutzer auf die zugeordneten Dateien durch Auswahl der Links zugreifen kann. Da jedoch die Dateien oft nicht von dem Suchanbieter, sondern von anderen Entitäten aufbewahrt und kontrolliert werden, hat der Suchanbieter typischerweise keinen Mechanismus zur Bestimmung der Virusrisiken, die von den Dateien präsentiert werden, die in Suchergebnissen identifiziert wurden, die an Nutzer der Suchmaschine geschickt wurden. Infolgedessen besitzen Dateien, auf die durch Ergebnisse von Suchmaschinen zugegriffen wird, oft für Nutzer einen vergleichsweise höheren Risikograd der Infektion. Falls insbesondere ein Nutzer keine lokale Anti-Virussoftware benutzt, ist solch ein Nutzer beträchtlich gefährdet, einen Virus einzufangen.

[0011] Der Wettbewerb zwischen kommerziellen Suchanbietern, gleichgültig ob diese Anbieter Suchsites oder Suchmaschinen, die von anderen genutzt werden, anbieten, ist relativ hart geworden, und demzufolge versuchen Suchanbieter kontinuierlich, die Zahl der Nutzer solcher Dienstleistungen zu erhöhen, speziell jene, wo der Ertrag hauptsächlich aus Werbung oder Mitgliedschaft herrührt. Viele Suchsites versuchen zum Beispiel, zusätzliche Funktionalität und Merkmale hinzuzufügen, um zusätzliche Nutzer zu bewe-

gen, ihre Dienste zu nutzen.

[0012] Unter der gegebenen harten Konkurrenz zwischen Suchanbietern wäre es sehr schädlich für einen Suchanbieter, auch nur entfernt als die Quelle eines Virus festgestellt zu werden, der in dem Computer des Nutzers Schaden anrichtet. Nichtsdestotrotz ist es oft unmöglich, bei dem Mangel an Kontrolle, die die meisten Suchanbieter über die Dateien haben, die von den Suchergebnissen identifiziert werden, die von solchen Anbietern oder deren Technologie erzeugt werden, auch nur ein marginales Niveau von Vertrauen zu schaffen, dass bestimmte Suchergebnisse kein beträchtliches Infektionsrisiko für Nutzer darstellen.

[0013] Die Risiken, die internetbasiertes Suchen birgt, können auch bei anderen Computer-Datenbanksuchumgebungen auftreten, speziell wenn die Möglichkeit besteht, dass Dateien, die gewissen Suchergebnissen zugeordnet sind, nicht unter der Steuerung der Entität stehen, die solche Suchergebnisse erzeugt. Deshalb besteht ein beträchtliches Bedürfnis im Fachgebiet nach einer Methode, Risiken von Viren zu verringern, die mit dem Zugreifen auf Suchergebnisse von Anfragen an Computerdatenbanken zusammenhängen.

Zusammenfassung der Erfindung

[0014] Die Erfindung befasst sich mit diesen und anderen Problemen, die mit dem bisherigen Stand der Technik zusammenhängen, indem in einem Aspekt ein System, ein Programmprodukt und ein Verfahren zur Verfügung gestellt werden, in denen die Funktionalität des Virusprüfens in eine Computerdatenbank-Suchumgebung integriert ist, um beim Schutz eines Nutzercomputers gegen das Zuziehen eines Computervirus beim Zugreifen auf Suchergebnisse zu helfen. Insbesondere beruht, entsprechend der Erfindung, die Erzeugung einer Bildschirmpräsentation einer Ergebnismenge, die als Antwort auf eine Suchanfrage erzeugt wurde, wenigstens zum Teil auf Virusstatusinformationen, die mit wenigstens einem Teil einer Vielzahl von Ergebnisdatensätzen zusammenhängen, die in der erzeugten Ergebnismenge identifiziert wurden.

[0015] Die wenigstens teilweise Zurückführung der Erzeugung der Bildschirmpräsentation auf die Virusstatusinformationen erlaubt es, die Ergebnismenge in einer Art und Weise anzuzeigen, die die Nutzerauswahl von Ergebnisdatensätzen, die ein höheres Virusrisiko darstellen könnten, verhindert. Zum Beispiel kann es in einigen Ausführungen erwünscht sein (und es sollte verstanden werden, dass eine große Vielzahl von alternativen Operationen ausgeführt werden kann), einfach das Anzeigen von Informationen wegzulassen, die mit Ergebnisdatensätzen zusammenhängen, von denen festgestellt wurde, dass sie ein Virusrisiko darstellen, wodurch effektiv verdächtige Suchergebnisse in einer Ergebnismenge eliminiert werden. Als Alternative kann es wünschenswert sein, Informationen der Anzeige, die mit verdächtigen Ergebnisdatensätzen zusammenhängen, hervorzuheben (zum Beispiel mit einem Icon oder einer anderen bestimmten Präsentation), um einen Nutzer zu informieren, dass solche Datensätze vergleichsweise höhere Virusrisiken darstellen. Weiterhin kann es wünschenswert sein, Informationen der Anzeige hervorzuheben (zum Beispiel mit einem Icon oder einer bestimmten Präsentation), die vertrauenswürdigen Ergebnisdatensätzen zugeordnet sind, um Nutzern eine gewisse Sicherheit zu geben, dass bestimmte Datensätze vergleichsweise geringere Virusrisiken bergen. Andere Anzeigemöglichkeiten werden für einen Fachmann offensichtlich sein, der den Nutzen dieser Offenbarung hat.

[0016] Die Erfindung befasst sich auch mit zusätzlichen Problemen, die mit der herkömmlichen Technik zusammenhängen, indem ein System, ein Programmprodukt und ein Verfahren zur Verfügung gestellt werden, in denen ein erster Computer konfiguriert ist, um Virusstatusinformationen zu empfangen, die von einer Vielzahl von Computern generiert wurden, wobei derartige empfangene Virusstatusinformationen in einer Virusdatenbank gespeichert werden, auf die der erste Computer zugreifen kann. Als eine Konsequenz können verschiedene Computer in der Lage sein, zuverlässige Virusstatusinformationen zur Nutzung durch einen gegebenen Computer zu generieren, wodurch erlaubt wird, die Verantwortlichkeit zur Erzeugung von Virusstatusinformationen genauso wie die verlangte Rechenstärke zur Erzeugung der Virusstatusinformationen auf verschiedene Computer zu verteilen. Durch die Verteilung der Verantwortlichkeiten zur Virusprüfung in dieser Art kann ein vergleichsweise größeres Volumen von Virusstatusinformationen erzeugt und/oder die Zeitnähe für Aktualisierungen existierender Virusstatusinformationen verbessert werden.

[0017] Diese und andere Vorteile und Merkmale, die die Erfindung charakterisieren, werden in den hier angefügten Ansprüchen erklärt und bilden einen weiteren Teil hiervon. Jedoch sollte, zum besseren Verständnis der Erfindung und der Vorteile und Ziele, die durch ihre Nutzung erreicht werden, auf die Zeichnungen und die begleitende Beschreibung, in der beispielhafte Ausführungsformen der Erfindung beschrieben sind, Bezug genommen werden.

Kurze Beschreibung der Zeichnungen

[0018] **Fig.** 1 ist ein Blockdiagramm eines Computersystems entsprechend der Erfindung.

[0019] **Fig.** 2 ist ein Flussdiagramm, das die Ausführung einer Suchroutine, die von der Suchmaschine von **Fig.** 1 ausgeführt wird, illustriert.

[0020] **Fig.** 3 ist ein Flussdiagramm, das den Programmfluss der Suchmaschine von **Fig.** 1 illustriert.

[0021] **Fig.** 4 ist ein Flussdiagramm, das den Programmfluss der Erweiterung zur Virusprüfung von **Fig.** 1 illustriert.

[0022] **Fig.** 5 ist ein Flussdiagramm, das den Programmfluss des Virusprüfers aus **Fig.** 1 illustriert.

[0023] **Fig.** 6 ist ein Flussdiagramm, das den Programmfluss der Steuerung der Virusprüfung von **Fig.** 1 illustriert.

[0024] **Fig.** 7 ist ein Diagramm einer beispielhaften Suchseite, die von der Suchmaschine aus **Fig.** 1 erzeugt wurde.

[0025] **Fig.** 8 ist ein Diagramm einer beispielhaften Suchergebnisseite, die von der Suchmaschine aus **Fig.** 1 erzeugt wurde.

Ausführliche Beschreibung

[0026] Wenn wir uns nun den Zeichnungen zuwenden, in denen gleiche Zahlen in den verschiedenen Ansichten gleiche Teile bezeichnen, dann veranschaulicht **Fig.** 1 ein Computersystem **10** entsprechend der Erfindung. Computersystem **10** ist als ein vernetztes Computersystem abgebildet, das eine Vielzahl von Computern oder Systemen **20, 30, 50** umfasst, die miteinander über ein Netzwerk **15** verbunden sind. Netzwerk **15** kann praktisch jede Art von Netzwerkverbindung repräsentieren, darunter (aber nicht darauf beschränkt) lokale Netzwerke (LAN), Weitverkehrsnetzwerke (WAN), drahtlose, öffentliche Netzwerke (zum Beispiel das Internet) und deren Kombinationen. Mehr noch, es wird verstanden werden, dass eine große Vielzahl von zusätzlichen Computern und anderen elektronischen Geräten durch das Netzwerk **15** vernetzt werden kann.

[0027] In der abgebildeten Umsetzung wird das Computersystem **10** hauptsächlich bei der Erzeugung und Ausgabe

von Datenbank-Suchergebnissen an einen Nutzer eingesetzt, insbesondere, um Webseiten und Websites, die über das Internet und/oder ein oder mehrere private Netzwerke unter Benutzung von eindeutigen Uniform Resource Locators (URLs) zugänglich sind, zu lokalisieren und auf sie zuzugreifen. In diesem Bereich wird Computer **20** typischerweise als ein Client oder Nutzercomputer eingesetzt, da er von einem Nutzer gebraucht wird, um eine Suchanfrage zu erzeugen und Suchergebnisse als Antwort auf solch eine Anfrage zu empfangen. Gleichermaßen wird Computer **30** typischerweise als ein Server realisiert, da er genutzt wird, um ankommende Suchanfragen von verschiedenen Nutzern zu verarbeiten, auf eine Computerdatenbank, zum Beispiel einen Webseitenindex oder ein Verzeichnis, als Antwort auf solche Suchanfragen zuzugreifen und Suchergebnisse an verschiedene Nutzercomputer, zum Beispiel Computer **20**, auszugeben. Computer **50**, der in größerer Ausführlichkeit weiter unten diskutiert wird, wird auch typischerweise als Servercomputer implementiert, da dieser Computer typischerweise genutzt wird, um geladene Dateien und andere potentiell virusverdächtige Computerdaten verschiedenen Nutzern anzubieten. Zusätzlich und besonders, falls die Entität, die einen der Computer **30** oder **50** besitzt, eine große kommerzielle Körperschaft ist (zum Beispiel eine große Suchsite oder Downloadsite im Internet), können Computer **30** oder **50** auch verschiedene, miteinander vernetzte Computer repräsentieren, die zum Beispiel als eine Gruppe oder ein Cluster arbeiten, die genutzt werden, um eine Website zu beherbergen und Suchergebnisse und/oder herunterladbare Dateien für Hunderte oder Tausende von Nutzern anzubieten.

[0028] Für die Zwecke der Erfindung kann jedes System **20, 30** und **50** praktisch jede Art von Computer, Computersystem oder einem anderen programmierbaren elektronischen Gerät repräsentieren, einschließlich eines Client-Computers, eines Servercomputers, eines tragbaren Computers, eines Handcomputers, einer eingebetteten Steuerung usw. Auf jedes System **20, 30** und **50** wird nachstehend als "Computer" Bezug genommen, obwohl beachtet werden sollte, dass der Ausdruck "System" auch andere passende programmierbare elektronische Geräte entsprechend der Erfindung umfassen kann.

[0029] Wie in **Fig.** 1 gezeigt wird, enthält jeder Computer **20, 30** typischerweise wenigstens einen Prozessor **21, 31**, der einem Speicher **22, 32** zugeordnet ist. Eine Anzahl zusätzlicher Komponenten **23–26** und **33–36** ist auch jedem Prozessor **21, 31** zugeordnet, wie weiter unten diskutiert werden wird. Die gleichen Komponenten wie die Komponenten **21–26** und **31–36** werden auch typischerweise in Computer **50** genutzt (der in vielen Fällen ähnlich wie Computer **30** konfiguriert ist), obgleich solche Komponenten in **Fig.** 1 weggelassen wurden, um die Abbildung zu vereinfachen.

[0030] Jeder Prozessor **21, 31** kann einen oder mehrere Prozessoren (zum Beispiel Mikroprozessoren) darstellen, und jeder Speicher kann die Direktzugriffs-Speichereinheiten (RAM) darstellen, die den Hauptspeicher des entsprechenden Computers **20, 30** umfassen sowie auch alle Stufen von Zusatzspeichern, zum Beispiel Cache-Speicher, nicht flüchtige oder Backup-Speicher (zum Beispiel programmierbare oder Flash-Speicher), Nur-Lese-Speicher usw. Zusätzlich kann jeder Speicher **22, 32** so betrachtet werden, als ob er einen Speicher enthält, der sich physisch irgendwo in dem entsprechenden Computer **20, 30** befindet, zum Beispiel einen beliebigen Cache-Speicher in einem Prozessor **21, 31** genauso wie jede Speichermöglichkeit, die als virtueller Speicher genutzt wird, zum Beispiel gespeichert auf einer Massenspeichereinheit **25, 35** oder auf einem anderen Computer, der entweder Computer **20** oder **30** über ein Netzwerk zugeordnet ist.

[0031] Jeder Computer **20, 30** empfängt typischerweise auch eine Anzahl von Eingaben oder Ausgaben, um Informationen extern weiterzugeben. Für eine Schnittstelle mit einem Nutzer oder Bediener beinhaltet jeder Computer **20, 30** typischerweise ein oder mehr Nutzereingabeeinheiten **23, 33** (unter Anderem zum Beispiel eine Tastatur, eine Maus, einen Trackball, einen Joystick, ein Touchpad und/oder ein Mikrofon) und eine Anzeige **24, 34** (unter Anderem zum Beispiel einen CRT-Monitor, eine LCD-Anzeige und/oder Lautsprecher).

[0032] Zur zusätzlichen Speicherung kann jeder Computer **20, 30** auch einen oder mehrere Massenspeicher **25, 35** umfassen, unter Anderem zum Beispiel ein Disketten- oder ein anderes entfernbares Laufwerk, eine Festplatte, einen Speicher mit Direktzugriff (DASD), ein optisches Laufwerk (zum Beispiel ein CD-Laufwerk, ein DVD-Laufwerk usw.) und/oder ein Bandlaufwerk. Weiterhin kann jeder Computer **20, 30** eine Schnittstelle **26, 36** zu einem oder mehreren Netzwerken umfassen (unter Anderem zum Beispiel ein LAN, ein WAN, ein drahtloses Netzwerk und/oder das Internet **15**), um die Kommunikation von Informationen mit anderen Computern, die mit dem Netzwerk zugeordnet sind, zu erlauben. Es sollte beachtet werden, dass jeder Computer **20, 30** typischerweise passende analoge und/oder digitale Schnittstellen zwischen den Prozessoren **21, 31** und jeder Komponente **22–26** und **32–36** besitzt, wie im Fachgebiet allgemein bekannt ist.

[0033] Jeder Computer **20, 30** arbeitet unter der Steuerung eines Betriebssystems **27, 38** und führt verschiedene Computersoftwareanwendungen, Komponenten, Programme, Objekte, Module, Datenstrukturen (zum Beispiel die Komponenten **28–29** in Computer **20** und die Komponenten **40–46** in Computer **30**, unter Anderem) aus oder hängt auf andere Art von ihnen ab. Darüber hinaus können verschiedene Anwendungen, Komponenten, Programme, Objekte, Module usw. auch auf einem oder mehreren Prozessoren eines anderen Computers ausgeführt werden, der entweder Computer **20** oder **30** über ein Netzwerk zugeordnet ist, zum Beispiel in einer verteilten oder einer Client-Server-Rechnerumgebung, wobei die Rechnerleistung, die erforderlich ist, um die Funktionen eines Computerprogramms umzusetzen, an verschiedene Computer über ein Netzwerk verteilt werden kann.

[0034] Im Allgemeinen werden die Routinen, die ausgeführt werden, um die Ausführungsformen der Erfindung zu implementieren, sei es als Teil eines Betriebssystems oder einer bestimmten Anwendung, einer Komponente, eines Programms, eines Objektes, eines Moduls oder einer Befehlsfolge, hier als "Computerprogramme" oder einfach als "Programme" bezeichnet. Die Computerprogramme umfassen typischerweise einen oder mehrere Befehle, die zu verschiedenen Zeiten in verschiedenen Speichern und Speichereinheiten in einem Computer vorhanden sind, und die, wenn sie von einem oder mehreren Prozessoren in einem Computer gelesen und ausgeführt werden, dazu führen, dass der Computer die Schritte ausführt, die notwendig sind, um die Schritte oder Elemente auszuführen, die die verschiedenen Seiten der Erfindung verkörpern. Weiterhin werden, obwohl die Erfindung bisher und auch nachstehend im Kontext voll funktionierender Computer und Computersysteme beschrieben ist, Fachleute erkennen, dass die verschiedenen Ausführungsformen der Erfindung als ein Programmprodukt in einer Vielzahl von Formen verteilt werden können und dass die Erfindung in gleicher Weise anwendbar ist, ungeachtet der speziellen Art der signaltragenden Medien, die zum eigentlichen Ausführen der Verteilung genutzt werden.

Beispiele für signaltragende Medien sind, ohne sich darauf zu beschränken, unter Anderem Medien vom beschreibbaren Typ, zum Beispiel flüchtige und nichtflüchtige Speichereinheiten, unter Anderem Disketten und andere entfernbare Platten, Festplatten, Magnetbänder, optische Platten (zum Beispiel CD-ROMs, DVDs usw.), und Übertragungsmedien, zum Beispiel digitale und analoge Kommunikationsverbindungen.

[0035] Zusätzlich können verschiedene hier beschriebene Programme auf der Grundlage der Anwendung identifiziert werden, für die sie in einer bestimmten Ausführungsform der Erfindung implementiert sind. Jedoch sollte beachtet werden, dass jede spezielle Programm-Nomenklatur, die folgt, nur aus Bequemlichkeit genutzt wird, und dass die Erfindung daher nicht einfach auf eine Verwendung in einer speziellen Anwendung beschränkt sein sollte, die von solch einer Nomenklatur identifiziert und/oder impliziert wird.

[0036] Fachleute werden erkennen, dass die in **Fig. 1** abgebildete Beispielsumgebung nicht beabsichtigt, die vorliegende Erfindung zu beschränken. Tatsächlich werden Fachleute erkennen, dass andere alternative Hardware- und/oder Softwareumgebungen genutzt werden können, ohne sich vom Umfang der Erfindung zu entfernen. Zum Beispiel kann die Erfindung Anwendung bei der Unterstützung der Bereitstellung von Virusschutz für praktisch jede Form von computerlesbaren Daten finden, auf die von einem Nutzer über Suchergebnisse, die als Antwort auf eine Suche in einer Computerdatenbank erzeugt werden, zugegriffen wird.

[0037] **Fig. 1** veranschaulicht auch die Hauptsoftwarebestandteile, die bei der Implementierung des Virusprüfens und -meldens für Suchergebnisse einer Computerdatenbank entsprechend der Erfindung genutzt werden. Wie oben besprochen, ist die abgebildete Umsetzung speziell konfiguriert, um Virusschutz zu gewährleisten, in Verbindung mit Suchergebnissen aus Dokumenten, Dateien oder anderen computerlesbaren Daten, die im Internet oder einer anderen Form eines öffentlichen oder privaten Netzwerkes gespeichert sind. Deshalb ist Computer **30** typischerweise als ein Webserver realisiert, der Suchfunktionalität zur Ausführung von Computerdatenbank-Suchoperationen umsetzt, die für den Zugriff auf in Netzwerken zugängliche Daten geeignet sind. Dateien, Dokumente und andere netzwerkzugängliche Daten, die dargestellt werden können und einem Nutzer über Suchergebnisse zugänglich sind, heißen hiernach gewöhnlich "Dateien", obgleich zu beachten ist, dass dieser Ausdruck allgemein auf praktisch jede Form von computerlesbaren Daten angewandt werden kann, so dass der Ausdruck gleichermaßen nicht auf eine bestimmte Datei, ein Dokument, eine Datenstruktur oder ein Datenbankformat beschränkt ist.

[0038] Um die oben beschriebene Suchfunktionalität sowie eine zusätzliche Virusprüfungs- und Virusmelde-Funktionalität entsprechend der Erfindung zu unterstützen, benutzt Computer **30** eine Anzahl von Softwarekomponenten, einschließlich einer Suchmaschine **40**, eines Webcrawler **42**, einer Virusprüfsteuerung **44** und einer Virusdatenbank **46**.

[0039] Die Suchmaschine **40** kann implementiert werden, indem eine beliebige Anzahl von bekannten Suchtechnologien benutzt wird, inklusive indexbasierter Suchmaschinen und/oder verzeichnisbasierter Suchmaschinen, die beide im Fachgebiet allgemein bekannt sind. Suchmaschine **40** wird jedoch erweitert, um die Erzeugung von Anzeigeinformationen für eine Ergebnismenge zu unterstützen, die wenigstens zum Teil auf Informationen zum Virusstatus beruhen, die in der Virusdatenbank **46** gespeichert sind.

[0040] Eine indexbasierte Suchmaschine greift typischerweise auf eine Computerdatenbank zu, die von einem Webcrawler oder einer anderen Komponente konstruiert wurde, und die auch Indexdatensätze enthält, die bestimmten Dateien zugeordnet sind, die Indizes nicht-trivialer Terme und/oder anderer Daten in den zugeordneten Dateien enthalten. Eine Suche, die auf einer indexbasierten Suchmaschine ausgeführt wird, beinhaltet allgemein eine Durchsuchung der Indexdatensätze in einer Computerdatenbank, um Datensätze zu lokalisieren, die einen oder mehr indizierte Terme haben, die mit Termen übereinstimmen, die in einer Suchanfrage spezifiziert wurden. Typischerweise umfasst jeder Indexdatensatz die dem Datensatz zugeordneten Indexterme und auch den Speicherort (zum Beispiel eine URL) der zugeordneten Datei. Zusätzliche Informationen, zum Beispiel eine Zusammenfassung des Dokumentes, können auch innerhalb eines Indexdatensatzes implementiert werden.

[0041] Eine verzeichnisbasierte Suchmaschine umfasst typischerweise eine Computerdatenbank, die von einer Gruppe von Forschern erzeugt wurde, die Dateien entsprechend dem Inhalt einordnen und solchen Dateien zugeordnete Datensätze erstellen, von denen jeder einen Speicherort und typischerweise einen Titel und eine Zusammenfassung der Inhalte der zugeordneten Datei umfasst. Die Datensätze sind in verschiedenen Kategorien organisiert, so dass Dokumente, die einen ähnlichen Inhalt haben, in die gleichen Kategorien eingeordnet werden.

[0042] Als Alternative können verschiedene alternative Suchtechnologien genutzt werden. Zum Beispiel kann Suchmaschine **40** verschiedene Suchtechnologien nutzen, um zum Beispiel sowohl auf eine indexbasierte Datenbank als auch auf eine verzeichnisbasierte Datenbank zuzugreifen. Zusätzlich wird verstanden werden, dass angesichts dessen, dass eine große Vielzahl von privaten Computernetzwerken internetbasierte Technologien nutzt (zum Beispiel wenn sie als Intranet und/oder Extranet implementiert sind), sich die Dateien, die in einer der Erfindung entsprechenden Computerdatenbank dargestellt werden, auf einem privaten Netzwerk oder sogar auf einem einzelnen Computer befinden können und auf sie über andere Speicherortidentifikationen als URLs zugegriffen werden kann.

[0043] Mehr noch, die Erfindung kann bei der Erzeugung von Suchergebnissen aus jeder anderen Art von Computerdatenbank anwendbar sein, bei denen ein Risiko existiert, einen Virus einzufangen, wenn auf Dateien zugegriffen wird, die Suchergebnissen zugeordnet sind.

[0044] Die nachstehende Diskussion wird sich auf zwei Hauptfunktionalitäten konzentrieren, die implementiert sind, um Virusschutz zur Verfügung zu stellen, der Computerdatenbank-Suchergebnissen entsprechend der Erfindung zugeordnet ist. Eine erste Funktionalität ist die des Zugreifens auf Informationen zum Virusstatus, die verschiedenen Ergebnisdatensätzen in einer Suchergebnismenge zugeordnet sind, um dabei zu helfen, einen Nutzer gegen das Einfangen eines Virus aus irgendeiner Datei zu schützen, die in der Suchergebnismenge dargestellt ist. Eine zweite Funktionalität ist der Aufbau einer Datenbank mit Informationen zum Virusstatus, die beim Prüfen von Suchergebnissen auf das Risiko einer Virusinfektion genutzt wird.

[0045] Die erste Funktionalität wird hauptsächlich in der veranschaulichten Ausführungsform implementiert, die Suchmaschine **40** nutzt. Die zweite Funktionalität, die des Erzeugens von Informationen zum Virusstatus, wird hauptsächlich in der dargestellten Ausführungsform implementiert, die den Web Crawler **42** und die Virusprüfsteuerung **44** im Computer **30** nutzt, sowie als Virusprüferweiterung **29** im Computer **20** und als Virusprüfkomponente **52** im Computer **50**.

[0046] Insbesondere wird verstanden werden, dass in vielen Beispielen die potentielle Anzahl der Dateien, auf die als Antwort auf eine Computersuchanfrage zugegriffen werden

kann, eine beträchtliche Größe besitzen kann, besonders im Fall von internetbasierten Dateien. Obwohl es in einigen Ausführungsformen möglich sein kann, die Virusprüfung von Dateien, die durch eine Ergebnismenge dargestellt werden, in Echtzeit auszuführen, nachdem die Ergebnismenge erzeugt ist (entweder durch die Suchmaschine oder durch einen Nutzercomputer), wäre in vielen Beispielen die Menge an Verarbeitungsleistung, die erforderlich ist, um ein solches Virussuchen auszuführen, jenseits der Möglichkeiten vieler Computer.

[0047] Deshalb ist es oft wünschenswert, viel von der Erzeugung von Informationen zum Virusstatus im Hintergrund auszuführen sowie wenigstens einen Teil der Verarbeitung, die dem Erzeugen solcher Statusinformationen zugeordnet ist, auf andere Computer zu verteilen, so dass auf existierende Informationen zum Virusstatus, falls verfügbar, zugegriffen werden kann, nachdem eine Ergebnismenge erzeugt ist, um das Melden oder eine andere Behandlung von potentiellen Quellen von Computerviren in einer Ergebnismenge zu beschleunigen.

[0048] Eine Methode zum Übertragen der Erzeugung von Informationen zum Virusstatus auf einen Hintergrundprozess besteht in der Benutzung des Webcrawlers **42**. Im Besonderen wird der Webcrawler **42** typischerweise als eine Erweiterung der konventionellen Webcrawler-Funktionalitäten implementiert, die gemeinhin zum Indizieren von Dateien bei der Erzeugung von Indexdatenbanken genutzt werden, insbesondere um die Virusprüfung als eine weitere Operation hinzuzufügen, die mit einer bestimmten Datei ausgeführt wird, während ein Webcrawler einen Indexdatensatz, der dieser Datei zugeordnet ist, erzeugt oder aktualisiert. Virusprüfung durch einen Webcrawler **42** wird genutzt, um Informationen zum Virusstatus zu erzeugen, die anschließend in einer Virusdatenbank **46** gespeichert und von der Suchmaschine **40** bei der Anzeige der Suchergebnisse genutzt werden.

[0049] In anderen Umsetzungen kann der Umfang der Dateien, die möglicherweise in einer Ergebnismenge dargestellt werden können, sogar die Fähigkeit eines Webcrawlers übersteigen, Informationen zum Virusstatus für einen großen Teil der Dateien zu liefern, die in irgendeiner speziellen Ergebnismenge dargestellt werden (wobei es klar ist, dass es das vorrangige Ziel von vielen Webcrawlern ist, zu versuchen so viel wie möglich vom Internet abzudecken). Deshalb ist es oft wünschenswert, entsprechend der Erfindung, weiterhin einige der Verantwortlichkeiten zur Ausführung von Virusprüfungen an entfernte Computer zu delegieren und sich dann auf die Kommunikation von diesen entfernten Computern zu verlassen, um Informationen zum Virusstatus, die in der Virusdatenbank **46** gespeichert werden, zu erzeugen. In der abgebildeten Umsetzung wird die Koordination solcher Aktivitäten durch die Virusprüfsteuerung **44** in Computer **30** durchgeführt.

[0050] Die Verantwortung zum Ausführen von Virusprüfungen kann zum Beispiel zu einem gewissen Teil an die aktuellen Nutzer der Suchmaschine delegiert werden. Wie in **Fig.** 1 veranschaulicht, kann ein Nutzercomputer **20** zum Beispiel eine Erweiterung zur Virusprüfung **29** beinhalten, die in Verbindung mit einem konventionellen Browser **28** arbeitet, um die Virusprüfung von Dateien, auf die ein Nutzer zugreift, auszuführen, wobei die Ergebnisse solcher Operationen an den Computer **30** zurückgeschickt und von der Virusprüfsteuerung **44** zur Aufnahme der zugeordneten Informationen zum Virusstatus in die Virusdatenbank **46** verarbeitet werden.

[0051] Noch eine andere Methode des Delegierens der Verantwortung für die Virusprüfung kann durch andere, dritte Computer geliefert werden, inklusive solcher von dritten Parteien, die nicht aktuell Nutzer der Suchmaschine sind. Eine solche Funktionalität wird in **Fig.** 1 durch den Virusprüfer **52** veranschaulicht, der die Virusprüfung von Dateien ausführt, die dem Computer **50** zugänglich sind, und Informationen zum Virusstatus zurück an die Virusprüfsteuerung **44** zur Aufnahme solcher Informationen in die Datenbank **46** meldet.

[0052] Der Virusprüfer **52** wird typischerweise genutzt, um Dateien zu prüfen, die von Computer **50** verwaltet werden oder ansonsten unter der Verantwortung von Computer **50** stehen, entweder aufgrund von Kopien der Dateien, die im Computer vorhanden sind, oder weil die Dateien mit anderen Dateien, die im Computer vorhanden sind, direkt verknüpft sind und/oder auf andere Weise durch sie angesprochen werden. Computer **50** kann zum Beispiel eine Website beherbergen, beispielsweise eine Site zum Herunterladen, die eine Anzahl von abrufbaren Dateien beinhaltet, die für Nutzer über das Internet zugänglich sind. Websites und insbesondere Sites zum Herunterladen und Ähnliches führen oft eine Virusprüfung im normalen Geschäftsverlauf aus, indem konventionelle Technologie zum Virussuchen benutzt wird. Im Gegensatz zu solchen internen Virusschutzmaßnahmen jedoch unterstützt der Virusprüfer **52** die zusätzliche Funktionalität des Meldens von Ergebnissen solcher Virusprüfungen an die Virusprüfsteuerung **44** zur Aufnahme der sich ergebenden Statusinformationen in die Datenbank **46**.

[0053] Während praktisch jede Art von Website oder eine andere Dateiquelle durch den Virusprüfer **52** bearbeitet werden kann, besteht eine besonders nützliche Anwendung in der Benutzung in Verbindung mit einer Site zum Herunterladen, die regelmäßig Nutzerzugang zu einer großen Vielzahl von herunterladbaren Softwareanwendungen und anderen Dateien gewährt, die eine vergleichsweise höhere Anfälligkeit für Virusinfektion haben. Ausführbare Dateien und auch Dateien, die auf Scripte und/oder ausführbare Objekte zugreifen, sowie komprimierte Dateien, die eine oder mehr dieser Arten von Dateien enthalten, sind besonders anfällig für eine Infektion, und deshalb ist es oft wünschenswert, Virusschutz in Verbindung mit einer Website zu liefern, die Nutzerzugang zu einer großen Zahl solcher Dateien gewährt.

[0054] Wie weiter unten noch offensichtlicher werden wird, kann der Virusprüfer **52**, zusätzlich zum Prüfen von Dateien, die von Computer **50** verwaltet werden, auch zusätzliches Virusprüfen unter der direkten Steuerung durch die Virusprüfsteuerung **44** ausführen und die Ergebnisse rechtzeitig zurück an die Virusprüfsteuerung melden. Eine ähnliche Funktionalität kann, falls gewünscht, auch in der Erweiterung **29** umgesetzt werden. Dies erlaubt es der Steuerung **44**, die Virusprüfung bestimmter Dateien an andere Computer zu delegieren und dadurch die Erzeugung zusätzlicher Informationen zum Virusstatus zu erleichtern.

[0055] Nimmt man beispielsweise an, dass eine Vielzahl von Nutzercomputern und Computern dritter Parteien zu verschiedenen Zeiten elektronisch Computer **30** zugeordnet sind, dann wird es verständlich sein, dass der Erzeugung von Informationen zum Virusstatus in der hier beschriebenen Weise eine beträchtliche Menge an Verarbeitungsleistung zugeordnet werden kann. Als ein Ergebnis wird die Durchführbarkeit der Erzeugung von Informationen zum Virusstatus für einen großen Anteil von möglichen Suchergebnissen dramatisch erhöht. Es wird jedoch von einem Fachmann, der den Nutzen der Offenbarung hat, verstanden, dass Informationen zum Virusstatus in einigen Ausführungsformen allein durch Nutzercomputer, durch Suchmaschinencomputer oder durch Computer dritter Parteien erzeugt werden können und demzufolge die Erfindung nicht auf die Benutzung

aller drei oben diskutierten Verfahren beschränkt ist.

[0056] **Fig.** 2 zeigt detaillierter eine Beispielsausführung der Suchroutine **60**, die von der Suchmaschine **40** des Computers **30** ausgeführt wird, um Informationen zum Virusstatus in die Erzeugung von Suchergebnissen in Übereinstimmung mit der Erfindung einzubeziehen. In der veranschaulichten Ausführungsform erzeugt die Suchmaschine **40**, wenn eine Suche ausgeführt wird, typischerweise Suchergebnisse als Antwort auf eine Suchanfrage, wobei solche Suchergebnisse durch eine Ergebnismenge dargestellt werden, die eine Vielzahl von Datensätzen in einer Datenbank identifiziert, die ein durch die Suchanfrage bestimmtes Kriterium erfüllen. Weiterhin ist in der abgebildeten Ausführungsform jeder Datensatz in der Ergebnismenge einer bestimmten Datei zugeordnet (zum Beispiel durch Einbeziehen eines Speicherortes für diese Datei), auf die durch einen Nutzer durch die Suchergebnisse zugegriffen werden kann. Zum Beispiel ist bei einer internetbasierten Suchmaschine, beispielsweise der Suchmaschine **40**, jeder Datensatz einer besonderen, über das Internet oder anderweitig über ein Netzwerk zugänglichen Datei zugeordnet, und jeder Datensatz enthält typischerweise eine URL, die den Speicherort einer solchen zugeordneten Datei liefert. Andere Arten der Verknüpfung von Dateien mit Ergebnisdatensätzen können als Alternative genutzt werden.

[0057] Routine **60** beginnt in den Blöcken **62** und **64**, indem ein Viruskriterium und ein Suchkriterium von einem Nutzer erhalten werden.

[0058] Das vom Nutzer erhaltene Viruskriterium bestimmt typischerweise die Regel, wonach in einer Ergebnismenge dargestellte Dateien als "nicht vertrauenswürdig" anzuzeigen sind, d. h. als Träger eines vergleichsweise höheren Virusinfektionsrisikos. Das Viruskriterium kann zum Beispiel einfach darauf basieren, ob eine in einer Ergebnismenge dargestellte Datei einen Virus enthielt oder nicht. Das Viruskriterium kann auch bestimmen, ob eine Datei innerhalb eines vorbestimmten Zeitabschnittes auf Viren geprüft wurde, so dass Dateien, die als nicht mit einem Virus infiziert befunden wurden, aber für einen längeren Zeitabschnitt nicht geprüft wurden, immer noch als nicht vertrauenswürdig betrachtet werden. Das Viruskriterium kann auch bestimmen, ob eine Datei seit der letzten Ausführung einer Virusprüfung geändert wurde, so dass geänderte Dateien als nicht vertrauenswürdig betrachtet werden, bis sie erneut überprüft worden sind. Zusätzlich kann auch ein Zeitabschnitt bestimmt werden, in dem Dateien als frei von Virusinfektionen befunden wurden, so dass Dateien, von denen vorher angenommen wurde, dass sie ein größeres Risiko eines Virus darstellen, nach dem Ende einer ausreichenden Zeitperiode, in der keine Viren gefunden wurden, immer noch den Vertrauensstatus erhalten können.

[0059] Ein Viruskriterium kann auch bestimmen, welche zusätzlichen Dateien, falls überhaupt, geprüft werden müssen, um eine bestimmte Datei als virusfrei zu bestätigen. Eine Datei kann zum Beispiel als virusfrei definiert werden, falls der aktuelle Inhalt der Datei als frei von allen Viren befunden wurde. Als Alternative hierzu kann der Status einer Datei von dem Status von zusätzlichen Dateien, die dieser Datei zugeordnet sind, abhängen, und als solches kann von einer Datei verlangt werden, nur mit Dateien zugeordnet zu sein, die auch virusfrei sind, bevor diese Datei als vertrauenswürdig bestimmt werden kann.

[0060] Beispielsweise besteht bei vielen Sites zum Herunterladen der Großteil der herunterladbaren Dateien, die auf solchen Sites verfügbar sind, aus ausführbaren Dateien, und diese sind nicht geeignet zum Indizieren oder Suchen, aufgrund ihres maschinenlesbaren Inhaltes. Auf der anderen Seite sind solche Dateien typischerweise über Webseiten oder Dokumente zugänglich, die in einer textbasierten Sprache, zum Beispiel der Hypertext Markup Language (HTML), formatiert sind, die selbst indexierbar und suchbar ist, die aber aufgrund ihrer Natur gewöhnlich ein vergleichsweise geringeres Risiko einer Virusinfektion liefert. Nichtsdestotrotz wäre es allgemein unerwünscht, ein HTML-Dokument als vertrauenswürdig anzuzeigen, wenn es mit irgendeiner infizierten ausführbaren Datei verknüpft ist.

[0061] Deshalb ist es in vielen Fällen für ein Viruskriterium wünschenswert, um sich den Befürchtungen zuzuwenden, die mit Dateien höheren Risikos verbunden sind, zu bestimmen, wie zusätzliche Dateien, die mit einer besonderen Datei verknüpft sind, bei der Bestimmung der Vertrauenswürdigkeit dieser Datei analysiert werden. Ein Viruskriterium kann zum Beispiel eine Verknüpfungstiefe bestimmen, die die Anzahl der aufeinander folgenden Verknüpfungen darstellt, die von einer bestimmten, analysierten Datei aus durchlaufen werden müssen. Ein Viruskriterium kann auch festlegen, dass die zusätzlichen Dateien unter der Steuerung der gleichen Stelle wie die analysierte Datei sind, zum Beispiel indem die zu analysierenden verknüpften Dateien auf Dateien in der gleichen Domain beschränkt werden.

[0062] Das Abfragen eines Suchkriteriums von einem Nutzer, das eine von diesem Nutzer gemachte Suchanfrage darstellt, enthält typischerweise eine beliebige Anzahl bekannter Suchtechnologien, darunter beispielsweise Schlüsselwort-Suche, logische Suche, Suche in natürlicher Sprache usw. In der abgebildeten Umsetzung kann beispielsweise ein Suchkriterium von einem Nutzer über eine Suchseite (zum Beispiel im HTML-Format) erlangt werden, die dem Nutzer über die Suchmaschine angeboten wird, inklusive passender Eingabefelder, in die ein Nutzer Suchbegriffe eingeben kann. Die Aufgabe einer Suchanfrage wird typischerweise ausgeführt, indem eine auf der Suchseite verfügbare Anfrage-Schaltfläche (submit-button) ausgewählt wird. Jedoch können auch andere Methoden der Eingabe eines Suchkriteriums als Alternative genutzt werden.

[0063] In der abgebildeten Umsetzung können das Viruskriterium und das Suchkriterium von einem Nutzer über eine gemeinsame Suchseite eingegeben werden. Zusätzlich kann es erwünscht sein, andere Nutzerpräferenzen festzulegen, zum Beispiel wie die Anzeige von Suchergebnissen, die als nicht vertrauenswürdig bestimmt wurden, gehandhabt werden soll. Als Alternative können einige oder alle Virus- und Suchkriterien sowie beliebige zusätzliche Nutzerpräferenzen für einen Nutzer auf dem lokalen Computer des Nutzers zwischengespeichert werden, wobei wenigstens ein Teil von entweder einem oder beiden Blöcken **62** und **64** die Abfrage der lokalen Nutzereinstellungen vom lokalen Computer des Nutzers enthalten können. Zusätzlich können in einigen Ausführungsformen gewisse Aspekte des Virus- und Suchkriteriums sowie beliebige zusätzliche Nutzerpräferenzen von einem Nutzer modifizierbar sein, oder als Alternative können gewisse derartige Aspekte durch die Suchmaschine festgelegt und nicht durch einen Nutzer bestimmt werden.

[0064] Wir setzen mit Routine **60** fort; sobald ein Viruskriterium und ein Suchkriterium von einem Nutzer erhalten wurden, geht die Steuerung auf Block **66** über, um die Suche entsprechend dem Stand der Technik durchzuführen. Als ein Ergebnis der Suchausführung wird typischerweise eine Ergebnismenge erzeugt, die eine Vielzahl von Ergebnisdatensätzen identifiziert, die dem Suchkriterium entsprechen. Im Falle einer indexbasierten oder verzeichnisbasierten Suchmaschine beinhaltet eine Ergebnismenge typischerweise Identifikatoren einer Vielzahl von Index- oder Verzeichnisdatensätzen in der jeweiligen Datenbank, wobei jeder derartige Datensatz eine oder mehr Dateien identifiziert, zum

Beispiel über URLs, die in solchen Datensätzen gespeichert sind.

[0065] Im Block **68** wird als nächstes die Ergebnismenge durchsucht, um die jedem Ergebnisdatensatz zugeordnete URL zu erhalten, wobei jede derartige URL benutzt wird, um auf die Virusdatenbank **46** zuzugreifen, um zu versuchen, Informationen zum Virusstatus für jede der von der Ergebnismenge dargestellten Dateien zu finden. Für jeden gefundenen Datensatz in der Virusdatenbank wird die dortige Information zum Virusstatus mit dem Viruskriterium verglichen, um zu bestimmen, ob der zugeordneten Datei vertraut oder nicht vertraut werden kann, nicht infiziert (oder frei) von Computerviren zu sein. Jede von der Ergebnismenge dargestellte nicht vertrauenswürdige Datei wird dann von der Suchmaschine markiert, um ihren nicht vertrauenswürdigen Status widerzuspiegeln. Zusätzlich können Dateien, die keine zugeordneten Informationen zum Virusstatus haben, als nicht vertrauenswürdig markiert oder separat in der Ergebnismenge angezeigt werden.

[0066] Als nächstes erzeugt Block **70** eine Anzeige von wenigstens einem Teil der Ergebnismenge, die auf den Informationen zum Virusstatus für die Ergebnismenge und anderen zusätzlichen Nutzerpräferenzen, die weiter unten diskutiert werden, beruht. Block **70** bietet auch (d. h. überträgt) die Anzeigedarstellung dem Nutzer als Ergebnis der Suche an.

[0067] In der abgebildeten Ausführung zum Beispiel beinhaltet die Erzeugung einer Anzeigedarstellung der Ergebnismenge typischerweise die Generierung eines HTML-kompatiblen Dokumentes, zum Beispiel eine Suchergebnisseite, die Informationen anzeigt, die wenigstens einer Untermenge der Ergebnisdatensätze in der Ergebnismenge zugeordnet sind. Typischerweise beinhalten die Anzeigeinformationen für einen Ergebnisdatensatz einen Titel und eine URL für die zugeordnete Datei und oft einen Hypertextlink zu der URL, so dass ein Nutzer direkt zu der zugeordneten Datei steuern kann. Die Anzeigeinformationen können zusätzlich andere Informationen beinhalten, zum Beispiel eine Zusammenfassung oder einen Auszug der Datei, ein Datum für die Datei und/oder einen Grad der Relevanz für die Datei.

[0068] Außerdem wird, wie oben besprochen, in vielen Fällen nur ein Teil der Ergebnisdatensätze in dem HTML-Dokument dargestellt, mit zusätzlichen in dem Dokument zur Verfügung gestellten Hypertextlinks, um zu erlauben, dass zusätzliche Suchergebnisse angesehen werden können. Zum Beispiel kann eine Suchergebnisseite erzeugt werden, um die ersten fünfzig Ergebnisse anzuzeigen, mit bereitgestellten Links, um zusätzliche Gruppen von jeweils fünfzig Ergebnissen auszuwählen. Nutzerpräferenzen (zum Beispiel wie in den lokalen Einstellungen auf dem lokalen Computer des Nutzers gespeichert oder auf einer Suchseite bestimmt) können auch bei der Bestimmung benutzt werden, wie die Anzeigedarstellung der Suchergebnisse zu formatieren ist.

[0069] Die Erzeugung der Anzeigedarstellung basiert, in Übereinstimmung mit der Erfindung, wenigstens zum Teil auf den Informationen zum Virusstatus, die für eine oder mehr Ergebnisdatensätze in der Ergebnismenge abgefragt wurden. Die Anzeigedarstellung kann zum Beispiel so erzeugt werden, dass jegliche Anzeigeinformationen wegzulassen sind, die Ergebnisdatensätzen zugeordnet sind, von denen festgestellt wurde, dass sie ein Risiko einer Virusinfektion darstellen. Als Alternative können die Anzeigeinformationen für Ergebnisdatensätze, von denen festgestellt wurde, dass sie ein Risiko einer Virusinfektion darstellen, in der Anzeigedarstellung hervorgehoben werden, zum Beispiel durch das Bereitstellen eines speziellen Icons im Zusammenhang mit der Anzeigeinformation oder durch wechselnde Methoden zur Hervorhebung, zum Beispiel die Benutzung von bestimmten Anzeigemerkmalen (zum Beispiel fett, kursiv usw.), vergrößerte Schrift, bestimmte Anzeigefarbe, Animation usw., oder durch die Benutzung einer Dialogbox oder andere aufklappende Fenster, eine Textbenachrichtigung irgendwo auf der Suchergebnisseite usw. Zusätzlich kann dem Nutzer ein hörbares Signal, zum Beispiel ein "Beep" oder ein anderes Geräusch, vorgespielt werden, um den Nutzer über ein potentielles Risiko zu benachrichtigen.

[0070] Weiterhin kann ein Nutzer immer dann gewarnt werden, wenn der Nutzer mit den Anzeigeinformationen arbeitet, die einem Risikoergebnisdatensatz zugeordnet sind, zum Beispiel bei Auswahl, oder selbst wenn ein Zeiger in der Nähe der Anzeigeinformationen oder einem Hypertextlink darin positioniert wird. Solch eine Warnung kann zum Beispiel durch jeder der oben beschriebenen Markierungstechniken sowie durch eine große Vielzahl von anderen Meldungstechniken geliefert werden.

[0071] Andere Arten von Audio- und/oder visuellen Techniken können in eine Anzeigedarstellung einer Ergebnismenge aufgenommen werden, um potentielle Risiken aufgrund von Viren anzuzeigen, wie von einem Fachmann erkannt wird, der den Nutzen dieser Offenbarung hat.

[0072] Zusätzlich zu oder anstatt der Hervorhebung von Anzeigeinformationen für nicht vertrauenswürdige Ergebnisdatensätze kann es wünschenswert sein, Anzeigeinformationen für Ergebnisdatensätze hervorzuheben, die Dateien zugeordnet sind, denen niedrige Risiken von Computerviren zugetraut werden, zum Beispiel über Icons oder jeden anderen oben beschriebenen Anzeigemechanismus. Zum Beispiel kann es erwünscht sein, ein Icon "bestätigt" bei den Anzeigeinformationen anzuzeigen, die einem bestimmten Ergebnisdatensatz, der als vertrauenswürdig befunden wurde, zugeordnet sind.

[0073] Es kann auch erwünscht sein, verschiedene Grade von Vertrauenswürdigkeit zu definieren und getrennt Ergebnisdatensätze auszuweisen, die solchen verschiedenen Graden entsprechen. Zum Beispiel kann es erwünscht sein, Dateien separat auszuweisen, für welche keine Informationen zum Virusstatus verfügbar sind. Als Alternative können alle solche Dateien als nicht vertrauenswürdig betrachtet werden, gemeinsam mit jenen, von denen festgestellt wurde, dass sie ein höheres Risiko einer Virusinfektion darstellen. Ebenso können Dateien, die noch nie einen Virus hatten, von Dateien unterschieden werden, die für einen bestimmten Zeitraum infektionsfrei gewesen sind.

[0074] Es wird zu erkennen sein, dass als Alternative eine große Vielzahl von weiteren Mechanismen benutzt werden können, die einen Nutzer vom Zugriff auf eine Datei abhalten, die einem Ergebnisdatensatz zugeordnet ist, der ein vergleichsweise höheres Risiko einer Virusinfektion hat. Deshalb ist die Erfindung nicht auf bestimmte, hier beschriebene Mechanismen beschränkt.

[0075] Wir wenden uns nun **Fig.** 3–6 zu; die verschiedenen Mechanismen, die genutzt werden können, um Informationen zum Virusstatus in der Virusdatenbank **46** zu erzeugen, werden nachstehend in größerer Ausführlichkeit beschrieben. Wie oben besprochen wurde, ist eine mögliche Quelle für Informationen zum Virusstatus in der Virusdatenbank **46** der Webcrawler **42**, dessen Programmablauf in größerer Ausführlichkeit in **Fig.** 3 illustriert ist.

[0076] Der Webcrawler **42** beginnt im Block **80** mit dem Erhalt einer neuen, zu prüfenden URL. Typischerweise geschieht die Auswahl einer neuen URL in Block **80** über ein Webcrawling-Protokoll, wie es für viele Webcrawler üblich ist. Das Erlangen einer neuen URL zum Beispiel kann über die Auswahl einer URL geschehen, auf die in einem Hypertextlink in einer vorher bearbeiteten Datei Bezug genommen wurde.

[0077] Nach dem Erhalt einer neuen URL geht die Steuerung zu Block **82** über, um zu bestimmen, ob sich die URL geändert hat – das heißt, ob die durch die URL ausgewiesene Datei aktualisiert wurde, nachdem die Datei das letzte Mal auf Viren überprüft worden ist. Typischerweise wird Block **82** implementiert, indem eine Prüfsumme, zum Beispiel eine CRC, von der Datei, auf die sich die URL bezieht, geliefert und die Prüfsumme mit der in der Datenbank **46** für die URL gespeicherten (falls solch ein Datensatz existiert) verglichen wird. Wechselnde Arten der Bestimmung, ob eine Datei seit einem früheren Zeitpunkt aktualisiert wurde, können auch als Alternative genutzt werden, zum Beispiel der Vergleich eines laufenden Zeitstempels mit einem Revisionsdatum, das Absuchen der Inhalte der Datei und durch andere in der Technik bekannte Formen. Alternativ kann der Status der Aktualisierung einer Datei in anderen Ausführungsformen nicht analysiert werden, wodurch Block **82** weggelassen würde.

[0078] Falls die URL als nicht geändert festgestellt wurde, geht die Steuerung auf Block **84** über, um zu bestimmen, ob die URL auf Viren geprüft wurde. Typischerweise wird Block **84** implementiert, indem auf den Datensatz (fall vorhanden), der der URL in der Virusdatenbank **46** zugeordnet ist, zugegriffen wird, um zu bestimmen, ob der URL Informationen zum Virusstatus zugeordnet sind.

[0079] Falls entweder Block **82** bestimmt, dass die URL geändert wurde, oder Block **84** bestimmt, dass die ULR vorher nicht auf Viren geprüft wurde, geht die Steuerung auf Block **86** über, um eine FOR-Schleife zur Ausführung einer Virusprüfung für die URL einzuleiten. Block **86** bearbeitet speziell jede virusverdächtige Datei, die von der URL aus zugänglich ist. In Abhängigkeit von der speziellen benutzten Technik zum Virussuchen können entweder nur ausführbare Dateien analysiert werden, oder als Alternative können alle Dateien, inklusive komprimierter Dateien, Dateien mit Daten und/oder die bestimmte, unter der URL gespeicherte Datei, geprüft werden. Darüberhinaus kann, wie oben besprochen, ein Parameter zur Linktiefe genutzt werden, um zu bestimmen, wie viele Links zu durchlaufen sind, um die Vertrauenswürdigkeit der URL zu bestimmen.

[0080] Für jede derartige virusverdächtige Datei geht die Steuerung auf Block **88** über, um die Datei herunterzuladen, und dann zu Block **90**, um eine Virusprüfung mit der Datei durchzuführen, indem eine beliebige Zahl in der Technik bekannter konventioneller Techniken zum Virussuchen benutzt wird. Die Steuerung kehrt dann zu Block **86** zurück, um zusätzliche Dateien, die von der URL aus zugänglich sind, zu bearbeiten.

[0081] Sobald alle derartigen Dateien auf Viren überprüft wurden, gibt Block **86** die Steuerung an Block **92** weiter, um einen neuen Datensatz zu erzeugen oder einen existierenden Datensatz für die URL in der Virusdatenbank zu aktualisieren. Verschiedene Typen von Informationen zum Virusstatus können in einem URL-Datensatz in der Virusdatenbank gespeichert werden, darunter zum Beispiel der Virusstatus (ob ein Virus in irgendeiner zugänglichen Datei gefunden wurde), ein Zeitstempel (der anzeigt, wann die URL zum letzten Mal auf Viren geprüft wurde) und eine Prüfsumme (die benutzt wird, um zu bestimmen, ob die ULR bei einem zukünftigen Zugriff geändert wurde). Zusätzliche Informationen zum Virusstatus, zum Beispiel der Typ des gefundenen Virus, die Namen aller Dateien, die Viren enthalten usw., können auch in einem URL-Datensatz entsprechend der Erfindung, gespeichert werden.

[0082] Sobald der URL-Datensatz erzeugt oder aktualisiert wurde, geht die Steuerung auf Block **94** über, um konventionelle Webcrawling-Operationen für die URL auszuführen. Alternativ hierzu kann Webcrawler **42** keine zusätzlichen Funktionen außerhalb des Virusprüfens ausführen, wodurch Block **94** weggelassen werden kann. Ungeachtet dessen geht die Steuerung als nächstes zu Block **80** zurück, um eine neue URL zur Bearbeitung zu erhalten.

[0083] Wir kehren zu Block **84** zurück; falls für eine URL festgestellt wurde, dass sie nicht geändert und in der Vergangenheit virengeprüft wurde, geht die Steuerung auf Block **96** über, um festzulegen, ob die Virusprüfung der URL ausgelassen werden kann. Insbesondere bestimmt Block **96**, ob die URL zuletzt als nicht vertrauenswürdig befunden wurde, d. h. sich auf eine Datei bezieht, die einen Virus besitzt oder mit einer anderen Datei verlinkt ist, die einen Virus hat, indem auf den URL-Datensatz zugegriffen wird, der der URL in der Virusdatenbank zugeordnet ist, um zu bestimmen, ob die Informationen zum Virusstatus anzeigen, dass ein Virus während der letzten Virusüberprüfung der URL gefunden wurde.

[0084] Falls die URL nicht als nicht vertrauenswürdig befunden wurde, geht die Steuerung auf Block **98** über, um zu bestimmen, ob die Schwellwert-Zeit einer "guten" URL abgelaufen ist – das heißt, ob ein übermäßig großer Zeitraum vergangen ist, seit die URL zuletzt auf Viren geprüft wurde. Falls nicht, geht die Steuerung auf Block **94** über, wodurch die Virusprüfung der URL ausgelassen wird. Ansonsten geht die Steuerung auf Block **86** über, um eine Virusprüfung für die Datei in der oben besprochenen Weise auszuführen.

[0085] Wir kehren zu Block **96** zurück; falls die URL für nicht vertrauenswürdig befunden wurde, geht die Steuerung auf Block **99** über, um zu bestimmen, ob die Schwellwert-Zeit einer "schlechten" URL abgelaufen ist. Falls nicht, geht die Steuerung auf Block **94** über, um die Virusprüfung der URL zu umgehen. Ansonsten geht die Steuerung auf Block **86** über, um die URL erneut zu prüfen.

[0086] Es wird verstanden werden, dass die Schwellwert-Zeiten der "guten" URL und der "schlechten" URL empirisch bestimmt oder anderweitig eingestellt werden können, um sicherzustellen, das Informationen zum Virusstatus für die URLs in der Virusdatenbank relativ aktuell gehalten werden. Darüber hinaus können den "guten" und den "schlechten" URLs unterschiedliche Schwellwertzeiten zugeordnet werden, oder die gleiche Schwellwert-Zeit kann in beiden Fällen benutzt werden.

[0087] Wie oben besprochen – eine weitere Quelle von Informationen zum Virusstatus läuft über einen Nutzercomputer, zum Beispiel den Nutzercomputer **20** in **Fig.** 1. In der abgebildeten Implementation wird die Virusprüfung im Nutzercomputer über eine Erweiterung **29** eines Browsers **28** ausgeführt, das heißt eines konventionellen Browsers wie zum Beispiel der Internet Explorer der Microsoft Corporation oder der Navigator-Browser von Netscape Communications. Als Alternative kann die hier beschriebene Funktionalität der Virusprüfung direkt innerhalb eines Browsers implementiert werden oder innerhalb einer komplett davon getrennten Anwendung. Solch eine Funktionalität kann auch in Echtzeit an einen Nutzer geschickt werden, in Verbindung mit Suchergebnissen, das heißt über eine scriptbasierte oder ausführbare Objektumsetzung. Die Erfindung ist daher nicht auf die bestimmte, hier besprochene erweiterungsbasierte Umsetzung zur Virusprüfung beschränkt.

[0088] Die Erweiterung zur Virusprüfung **29** wird in größerer Ausführlichkeit in **Fig.** 4 abgebildet, deren Programmfluss in Block **110** beginnt, indem auf einen Befehl, eine bestimmte Datei auf Viren zu prüfen, vom Browser gewartet wird. Insbesondere ist Erweiterung **29** so konfiguriert, dass sie wartet, bis ein Nutzer versucht, eine virusverdächtige Datei, zum Beispiel eine ausführbare Datei oder eine Datei, die ein Script oder einen Link auf ein ausführbares Objekt enthält, herunterzuladen. Zusätzlich kann es in einigen Um-

setzungen erwünscht sein, die Erweiterung zu informieren, eine bestimmte Datei auf Viren zu prüfen, immer dann, wenn festgestellt wird, dass eine Datei sich auf andere Dateien bezieht, die anfällig für Virusinfektion sein können. Die Umsetzung einer solchen Funktionalität innerhalb des Browsers **28** und der Erweiterung **29** wären innerhalb der Fähigkeiten eines Fachmannes, der den Nutzen dieser Offenbarung hat, wobei typischerweise der Browser so konfiguriert ist, dass er überwacht, welche Dateien der Nutzer versucht herunterzuladen, und die Erweiterung benachrichtigt, wenn irgendwelche virusverdächtigen Dateien (zum Beispiel ausführbare Dateien) von einem Nutzer angefordert werden.

[0089] Immer wenn ein Befehl vom Browser empfangen wird, geht die Steuerung auf Block **112** über, um die URL für die Datei (oder alternativ die URL für die Datei, die sich auf diese Datei bezieht) zu erhalten. Block **114** prüft als Nächstes die Datei auf Viren, unter Benutzung konventioneller Techniken zum Virussuchen.

[0090] Block **116** bestimmt als Nächstes, ob ein Virus gefunden wurde. Falls ein Virus gefunden wurde, geht die Steuerung auf Block **118** über, um ein "schlechtes" Datenpaket zu bilden, das typischerweise den Namen der Datei, die zugeordnete URL und einen Zeitstempel enthält, der anzeigt, wann eine Virusprüfung für die Datei ausgeführt wurde. Zusätzlich können andere Informationen, zum Beispiel die Art des Virus, mit dem "schlechten" Datenpaket geliefert werden. Block **120** sendet als Nächstes das "schlechte" Datenpaket an die Virusprüfsteuerung, und Block **122** informiert optional den Nutzer, dass ein Virus gefunden wurde. Zusätzlich kann es erwünscht sein, dem Nutzer zu erlauben, eine Impfung der Datei auszuführen oder andere Meldefunktionalitäten auszuführen, die in der Technik des Virussuchens allgemein bekannt sind. Nach Beendigung von Block **122** kehrt die Steuerung zu Block **110** zurück, um weitere Dateien zu bearbeiten (falls vorhanden).

[0091] Wir kehren zu Block **116** zurück; falls kein Virus gefunden wird, geht die Steuerung direkt auf Block **110** über. Alternativ kann es in einigen Umsetzungen wünschenswert sein, ein "gutes" Datenpaket an die Virusprüfsteuerung zu schicken, falls kein Virus gefunden wird.

[0092] In der abgebildeten Umsetzung werden alle Datenpakete, die von der Erweiterung **29** an die Virusprüfsteuerung **44** geschickt werden, verschlüsselt und mit Informationen zur Authentifizierung versehen, so dass die Virusprüfsteuerung in der Lage ist, die Inhalte des Datenpaketes und dessen Absender zu beglaubigen, so dass nur vertrauenswürdige Datenpakete genutzt werden, um die Informationen zum Virusstatus in der Virusdatenbank zu aktualisieren. Zusätzliche Funktionalität kann in die Erweiterung **29** aufgenommen werden, um sicherzustellen, dass die Erweiterung nicht verändert wurde und dadurch eine böswillige Partei davon abzuhalten, zu versuchen, die Informationen zum Virusstatus in der Datenbank mit ungültigen Daten zu verfälschen. Deshalb müssen typischerweise immer, wenn die Erweiterung **29** an einen Nutzer verteilt wird, eventuell zusätzliche Autorisierungsmechanismen ausgeführt werden, zum Beispiel, um zu Beginn die Erweiterung bei der Virusprüfsteuerung zu registrieren.

[0093] **Fig. 5** illustriert den Programmfluss von noch einer anderen optionalen Quelle von Informationen zum Virusstatus, die des Virusprüfers **52**, der auf einem Computer Dritter, zum Beispiel einem Webserver oder einem Serverkomplex bereitgestellt wird. Der Virusprüfer **52** läuft in einer Endlosschleife, wobei er in Block **130** eine neue URL zum Prüfen erhält. Die Bestimmung, welche URL als nächstes zu prüfen ist, kann ausgeführt werden, indem eine beliebige Anzahl von Algorithmen benutzt wird, zum Beispiel durch Auswahl von URLs aus jeder Datei, die von der Website aus zugänglich ist. In einigen Umsetzungen kann auch eine Liste von URLs von einen Suchprovider zum Bearbeiten geliefert werden, als eine Form servicebasierter "Steuer" oder als Entgelt für die Erlaubnis, dass Nutzer einer Suchmaschine auf dem Computer von Dritten nach Dateien suchen und auf Dateien zugreifen.

[0094] Für jede dieser URL sendet Block **132** als Nächstes ein "Benachrichtigungs"(notify)-Datenpaket an die Virusprüfsteuerung, um anzuzeigen, dass der Virusprüfer eine Virusprüfung einer neuen URL einleitet. Die URL, die geprüft wird, wird optional in dem "Benachrichtigungs"-Datenpaket geliefert, obgleich in vielen Fällen keine URL geliefert werden muss, da der Grund des "Benachrichtigungs"-Datenpaketes ist, anzufordern, dass die Virusprüfsteuerung eine Zusatz-URL schickt, die vom Virusprüfer auf Viren geprüft wird.

[0095] Als Nächstes wird in Block **134** ein Kennzeichen auf "falsch" gesetzt. Das Kennzeichen funktioniert als ein Modusselektor, der benutzt wird, um dem Virusprüfer zu erlauben, abwechselnd in Block **130** ausgewählte (hier als intern bereitgestellte URLs bezeichnet) URLs und zusätzliche URLs zu prüfen, die dem Virusprüfer durch die Virusprüfsteuerung von Computer **30** (hier als extern gelieferte URLs bezeichnet) geliefert werden. Andere Mechanismen zum Planen von URL-Prüfungen, die intern vom Virusprüfer und extern von der Virusprüfsteuerung erzeugt werden, könne auch als Alternative genutzt werden, zum Beispiel, um das Laden von URLs, die von den entsprechenden Quellen geliefert wurden, zu variieren.

[0096] Block **136** prüft als Nächstes die URL auf Viren, indem eine FOR-Schleife eingeleitet wird, um jede virusverdächtige Datei, die von der URL aus zugänglich ist, zu bearbeiten. Für jede solche Datei lädt Block **138** die Datei, und Block **140** führt eine Virusprüfung der Datei aus und speichert das Ergebnis der Virusprüfung temporär. Es ist verständlich, dass das Laden der Datei in Block **138** eine Abfrage einer externen Quelle verlangen kann, oder alternativ hierzu kann eine Kopie der Datei auf Computer **50** gehalten werden, wodurch das Laden der Datei eine Abfrage der Datei vom lokalen Speicher beinhaltet.

[0097] Sobald jede virusverdächtige Datei bearbeitet wurde, gibt Block **136** die Steuerung an Block **142**, um zu bestimmen, ob irgendein Virus in einer von der URL aus zugänglichen Datei gefunden wurde. Falls ja, wird in Block **144** ein "schlechtes" Datenpaket gebildet, ähnlich dem von Erweiterung **29** gebildeten. Falls kein Virus gefunden wird, gibt Block **142** stattdessen die Steuerung an Block **146**, um ein "gutes" Datenpaket ähnlich dem oben in Verbindung mit der Erweiterung **29** beschriebenen zu bilden. Wenn die jeweilige Datenpaketart geschaffen ist, wird das Datenpaket an die Virusprüfsteuerung in Block **148** geschickt. Zusätzlich kann das Datenpaket verschlüsselt und mit einer digitalen Signatur versehen sein, wie es von der Virusprüfsteuerung zum Beglaubigen verlangt wird.

[0098] Sobald das Datenpaket gesendet wurde, geht die Steuerung auf Block **150** über, um zu bestimmen, ob das Kennzeichen auf "wahr" gesetzt ist (was anzeigt, dass eine extern gelieferte URL bearbeitet wird). Falls nicht (wie beim ersten Durchlauf der Routine), geht die Steuerung auf Block **152** über, um eine extern gelieferte URL von der Virusprüfsteuerung abzufragen. Block **154** setzt dann das Kennzeichen auf "wahr", und Block **156** bestimmt, ob eine neue URL von der Virusprüfsteuerung erhalten wurde. Falls ja, kehrt die Steuerung zu Block **136** zurück, um jede virusverdächtige Datei, die von dieser URL aus zugänglich ist, auf Viren zu prüfen. Falls in Block **156** keine URL erhalten wird oder falls das Kennzeichen in Block **150** schon auf

"wahr" gesetzt ist, kehrt die Steuerung zu Block **130** zurück, um eine andere intern gelieferte URL, die geprüft werden soll, abzufragen. Es kann daher gesehen werden, dass die abgebildete Umsetzung des Virusprüfers **52** zwischen intern gelieferten und extern gelieferten URLs wechselt. Alternativ können dem Virusprüfer **52** keine extern gelieferten URLs bereitgestellt werden, wodurch eine solche darauf bezogene Funktionalität in **Fig.** 5 weggelassen werden kann.

[0099] **Fig.** 6 illustriert den Programmfluss der Virusprüfsteuerung **44** in größerer Ausführlichkeit. Im Allgemeinen ist die Virusprüfsteuerung **44** konfiguriert, in einer Endlosschleife zu arbeiten, um ankommende Datenpakete von allen autorisierten Virusprüferweiterungen und Virusprüfern, die für die Virusprüfsteuerung zugänglich sind, zu bearbeiten. Virusprüfsteuerung **44** beginnt mit dem Warten auf ein nächstes Datenpaket in Block **160**, das von einer externen Quelle empfangen werden soll. Als Antwort auf den Empfang eines solchen Datenpakets geht die Steuerung auf Block **162** über, um die Authentizität des Datenpakets zu überprüfen. Zum Beispiel kann es erwünscht sein, eine Datenbank von autorisierten Virusprüferweiterungen und/oder Virusprüfern zu unterhalten und auf die Datenbank zuzugreifen, um zu bestimmen, ob ein ankommendes Datenpaket ein authentisches Datenpaket ist, das von einem autorisierten Nutzer empfangen wurde. Eine beliebige Zahl konventioneller Sicherheitstechniken, zum Beispiel Public-Key-Verschlüsselung und/oder digitale Signaturen können benutzt werden. Darüber hinaus kann es in Block **162** erwünscht sein, das Datenpaket zu entschlüsseln, falls bei dem Datenpaket Verschlüsselung verwendet wurde.

[0100] Falls das Datenpaket als nicht authentisch bestimmt wird, geht die Steuerung von Block **164** auf Block **160** über, um auf ein nächstes Datenpaket zu warten, wodurch das aktuelle Datenpaket effektiv verworfen wird. Falls jedoch das Datenpaket als authentisch bestimmt wird, übergibt Block **164** die Steuerung an Block **166**, um zu bestimmen, ob das Datenpaket ein "Benachrichtigungs"-Datenpaket von einem Virusprüfer ist. Wie oben in Verbindung mit **Fig.** 5 besprochen wurde, wird ein "Benachrichtigungs"-Datenpaket benutzt, um die Virusprüfsteuerung zu alarmieren, dass ein bestimmter Virusprüfer bereit ist, eine extern gelieferte URL zu empfangen, um zusätzliches Virusprüfen auszuführen, sobald die Virusprüfung einer aktuellen, intern gelieferten URL abgeschlossen ist. Deshalb gibt Block **166**, als Antwort auf solch ein Datenpaket, die Steuerung an Block **168** ab, um die Virusdatenbank nach einer URL zu durchsuchen, die bald ausläuft – das heisst, eine URL, die einen Zeitstempel hat, der eine vorher bestimmte Schwelle überschreitet, die anzeigt, dass die URL erneut geprüft werden muss. Zusätzlich kann es erwünscht sein, URLs den Vorrang zu geben; auf die häufiger zugegriffen wird als auf andere URLs, und dadurch die Wahrscheinlichkeit zu maximieren, dass eine besondere URL, die als Antwort auf eine Suchanfrage abgefragt wurde, auf Viren geprüft wurde. Jede beliebige Anzahl von konventionellen Techniken zum Unterhalt einer Aufzeichnung der relativen Häufigkeit, in der auf bestimmte URLs zugegriffen wird, kann in Verbindung mit Block **168** benutzt werden.

[0101] Block **170** bestimmt als nächstes, ob eine passende URL gefunden wurde. Falls ja, geht die Steuerung auf Block **172** über, um die URL an den Virusprüfer zu senden, typischerweise, indem ein verschlüsseltes Datenpaket, das die URL enthält, an den Virusprüfer geschickt wird. Die Steuerung kehrt dann zu Block **160** zurück, um auf weitere Datenpakete zu warten.

[0102] Wir kehren nun zu Block **170** zurück; falls keine passende URL gefunden wurde, geht die Steuerung auf Block **174** über, um "keine URL" an den anfordernden Virusprüfer zu senden, zum Beispiel indem ein Datenpaket an den Virusprüfer geschickt wird, das anzeigt, dass keine URL verfügbar ist. Die Steuerung kehrt dann zu Block **160** zurück.

[0103] Wir kehren zu Block **166** zurück; falls das empfangene Datenpaket kein "Benachrichtigungs"-Datenpaket ist, geht die Steuerung auf Block **176** über, um zu bestimmen, ob das Datenpaket ein "schlechtes" Datenpaket ist, das von einer Virusprüferweiterung empfangen wurde. Falls ja, geht die Steuerung auf Block **178** über, um den URL-Datensatz zu aktualisieren, der der in dem Datenpaket bestimmten URL zugeordnet ist, um anzuzeigen, dass die URL nicht vertrauenswürdig ist. Zusätzlich werden solche Informationen, falls zusätzliche Informationen, zum Beispiel ein Zeitstempel und/oder die Identität von infizierten Dateien in dem Datenpaket vorhanden sind, in den Informationen zum Virusstatus für die URL gespeichert. Darüber hinaus kann dafür ein neuer Datensatz in der Virusdatenbank geschaffen werden, falls kein URL-Datensatz existiert. Die Steuerung kehrt dann zu Block **160** zurück, um zusätzliche Datenpakete zu bearbeiten.

[0104] Wir kehren zu Block **176** zurück; falls das Datenpaket kein "schlechtes" Datenpaket von einer Virusprüferweiterung ist, geht die Steuerung auf Block **180** über, um zu bestimmen, ob das Datenpaket ein "schlechtes" Datenpaket von einem Virusprüfer ist. Falls ja, geht die Steuerung auf Block **178** über, um einen Datensatz in der Virusdatenbank, der der in dem Datenpaket bestimmten URL zugeordnet ist, zu aktualisieren oder neu anzulegen. Und zu Block **180** zurückkehrend – falls das Datenpaket kein "schlechtes" Datenpaket von einem Virusprüfer ist, wird angenommen, dass das Datenpaket ein "gutes" Datenpaket von einem Virusprüfer ist, und die Steuerung geht daher auf Block **182** über, um einen URL-Datensatz in der Virusdatenbank für die dem Datenpaket zugeordnete URL zu aktualisieren oder neu anzulegen, was anzeigt, dass die URL als vertrauenswürdig befunden wurde, und was typischerweise einen Zeitstempel beinhaltet, der anzeigt, wann die Vertrauenswürdigkeit der URL durch eine Virusprüfung bestimmt wurde. Die Steuerung kehrt dann zu Block **160** zurück.

[0105] Als ein Beispiel für eine mit dem Computersystem **10** von **Fig.** 1 ausgeführte Suchoperation zeigt **Fig.** 7 ein Browserfenster **200**, das dem Browser **28** von Computer **20** zugeordnet ist und eine Suchseite **202** anzeigt, die von Suchmaschine **40** von Computer **30** erzeugt wurde. In der Suchseite ist es einem Nutzer erlaubt, ein Suchkriterium in ein Eingabefeld **204** einzugeben, wobei eine Suchanfrage erzeugt wird als Antwort auf die Auswahl eines Suchbuttons **206**, wenn er von einem Nutzer ausgewählt wurde. Zusätzlich wird verstanden, dass es erwünscht sein kann, zusätzliche Suchfähigkeiten für erweiterte Suche bereitzustellen, zum Beispiel über eine Seite für erweiterte Suche, die über einen Hypertextlink **208** zugänglich ist.

[0106] Die Suchseite **202** erlaubt es einem Nutzer auch, ein Viruskriterium einzugeben, zum Beispiel wie in Abschnitt **210** gezeigt, um es einem Nutzer zu erlauben, die Regel festzulegen, die benutzt wurde, um zu bestimmen, ob einer Datei zugetraut wird, mit einem geringen Risiko für einen Computervirus behaftet zu sein. Checkbox **212** erlaubt es beispielsweise einem Nutzer, festzulegen, dass eine Datei als nicht vertrauenswürdig bestimmt wird, falls jemals der Datei ein Virus zugeordnet war. Checkbox **214** erlaubt einem Nutzer, zu verlangen, dass eine Datei als nicht vertrauenswürdig bestimmt wird, falls ein Virus innerhalb einer vorbestimmten Zeitperiode gefunden wurde, zum Beispiel innerhalb einer vom Nutzer wählbaren Anzahl von Tagen. Checkbox **216** erlaubt einem Nutzer, zu verlangen, dass eine Datei als nicht vertrauenswürdig bestimmt wird, falls die

Datei innerhalb einer vorbestimmten Zeitperiode nicht überprüft wurde, zum Beispiel innerhalb einer vom Nutzer wählbaren Anzahl von Tagen. Zusätzliche Viruskriterien, zum Beispiel eine Linktiefe oder irgendwelche anderen oben besprochenen Alternativen, können auch in Abschnitt **210** dargestellt werden.

[0107] Es kann auch erwünscht sein, auf Suchseite **202** Eingaben für Nutzerpräferenzen zur Verfügung zu stellen, zum Beispiel die in Abschnitt **218** abgebildeten Meldeoptionen. Die Meldeoptionen legen fest, wie die Darstellung der Anzeige der Suchresultate erzeugt wird, auf der Grundlage der Bestimmung der Vertrauenswürdigkeit, die unter Benutzung des bestimmten Viruskriteriums vorgenommen wurde. Zum Beispiel zeigt die Auswahl von Radiobutton **220** an, dass ein Nutzer wünscht, alle dem Viruskriterium entsprechenden Ergebnisdatensätze auszulassen, so dass keine Anzeigeinformation für den Ergebnisdatensatz in den Suchergebnissen angezeigt wird. Radiobutton **222** erlaubt es einem Nutzer alternativ, über alle Ergebnisdatensätze informiert zu werden, die dem Viruskriterium entsprechen. Radiobutton **224** erlaubt es einem Nutzer, jede Meldung von Informationen zum Virusstatus in den zurückgegebenen Suchergebnissen auszuschalten. Andere Meldeoptionen, zum Beispiel die Art der Markierung, ob nicht vertrauenswürdige und/oder vertrauenswürdige Ergebnisse zu markieren sind usw., können auch von einem Nutzer auf Suchseite **202** entsprechend der Erfindung geliefert werden.

[0108] **Fig.** 8 illustriert als nächstes eine Beispielseite für Suchergebnisse **230**, die von der Suchmaschine als Antwort auf eine Suchanfrage erzeugt wurde, die von dem Nutzercomputer an die Suchmaschine weitergeleitet wurde. In den Beispielsuchergebnissen wird die den drei Ergebnisdatensätzen zugeordnete Anzeigeinformation in **232**, **234** und **236** abgebildet.

[0109] Angenommen, dass aus Beispielsgründen, die "Fred's PDA Download" und "Bill's PDA Links" genannten Ergebnisdatensätze entsprechend des nutzergewählten Viruskriteriums für nicht vertrauenswürdig befunden wurden und dass der Nutzer festgelegt hat, dass er oder sie über nicht vertrauenswürdige Ergebnisse informiert werden soll. Eine Umsetzung einer Suchergebnisseite kann daher in der Anzeige von Icons **238**, angrenzend oder nahe an den Anzeigeinformationen **234**, **236**, resultieren, um so einen Nutzer zu informieren, dass die Dokumente nicht vertrauenswürdig sind. Alternativ und wie oben besprochen, können andere Mechanismen zur Hervorhebung der Anzeigeinformationen **234**, **236** benutzt werden, und zusätzlich zur oder anstelle der Hervorhebung der Anzeigeinformationen für nicht vertrauenswürdige Ergebnisse kann die Hervorhebung der Anzeigeinformationen für vertrauenswürdige Ergebnisse, zum Beispiel die den Anzeigeinformationen **232** zugeordneten, ausgeführt werden (zum Beispiel indem ein Icon "beglaubigt" benutzt wird oder wie in der Darstellung).

[0110] Eine zusätzliche Funktion, die unterstützt werden kann, ist die Fähigkeit, Informationen zum Virusstatus als Antwort auf eine Nutzereingabe anzuzeigen. Zum Beispiel veranschaulicht **Fig.** 8 eine Nutzerauswahl eines Icons **238**, das der Anzeigeinformation **236** über einen vom Nutzer zu bedienenden Zeiger **240** zugeordnet ist. Als Antwort auf eine auf Icon **238** gerichtete Nutzereingabe wird ein aufklappbares Fenster **242** angezeigt, das Anzeigeinformationen bezüglich zusätzlicher Informationen zum Virusstatus enthält, die der URL zugeordnet sind, zum Beispiel einen Zeitstempel und den Namen einer infizierten Datei. Die Nutzereingabe, die die Anzeige von Fenster **242** auslöst, kann das Drücken einer Maustaste oder alternativ, neben anderen Eingaben, einfach die Positionierung von Zeiger **242** über Icon **238** sein. Bei der großen Vielzahl von alternativen grafischen Komponenten für Nutzerschnittstellen, die auf einer Plattform zum Webbrowsen verfügbar sind, ist klar, dass eine unendliche Zahl von alternativen Mechanismen genutzt werden kann, um sowohl die Anzeige der Informationen zum Virusstatus auszulösen als auch solche Informationen entsprechend der Erfindung einem Nutzer zu präsentieren.

[0111] Verschiedene Modifikationen können bei den abgebildeten Ausführungsformen vorgenommen werden, ohne sich vom Sinn und Umfang der Erfindung zu entfernen. Zum Beispiel kann auch Virusprüfen in Echtzeit für Suchergebnisse ausgeführt werden, anstelle der Benutzung von vorher gespeicherten Informationen zum Virusstatus oder zusätzlich zu ihr. Eine solche Prüffunktionalität in Echtzeit kann zum Beispiel in einem separaten Thread in der Suchmaschine umgesetzt oder in einigen Umsetzungen lokal von einem Computer des Nutzers ausgeführt werden. Darüber hinaus kann Virusprüfung in Echtzeit bei allen Suchergebnissen ausgeführt werden, oder als Alternative kann Virusprüfung in Echtzeit nur für Suchergebnisse ausgeführt werden, denen entsprechende Informationen zum Virusstatus fehlen. Weiterhin kann in einigen Ausführungsformen Virusimpfung unterstützt werden, um infizierte Dateien oder Computer zu reparieren.

[0112] Die abgebildeten Ausführungsformen haben eine Anzahl einzigartiger Vorteile gegenüber konventionellen Techniken zur Virusprüfung. Indem zum Beispiel die Anzeige der Suchergebnisse auf der Grundlage der Vertrauenswürdigkeit dieser Ergebnisse modifiziert wird, können Nutzer davon abgehalten werden, möglicherweise Risikodateien anzusteuern und sich Computerviren einzufangen. Zusätzlich können die Informationen zum Virusstatus, die bei solchen Bestimmungen benutzt werden, oft vor der Erzeugung von Suchergebnissen generiert werden, so dass Virusprüfen in Echtzeit eingeschränkt oder ganz vermieden werden kann. Darüber hinaus kann die Zusatzbelastung, die der Erzeugung von Informationen zum Virusstatus zugeordnet ist, auf viele Computer verteilt werden, einschließlich denen von Nutzern, die eine Suchmaschine benutzen, sowie andere Computer Dritter, zum Beispiel jene, die dem Herunterladen und anderen Websites zugeordnet sind.

[0113] Die Implementierung des hier besprochenen Virusprüfens und -meldens kann, besonders wenn sie in Verbindung mit großen kommerziellen Unternehmen der Internetsuche benutzt wird, beträchtliche Vorteile liefern. Die Bereitstellung solcher Funktionalität stellt einen erhöhten Wert dar, der mehr Besuche von Nutzern und daher höhere Werbeeinnahmen und/oder Abonnementeinnahmen für abonnementbasierte Dienstleistungen begünstigt.

[0114] Zusätzlich erhöht (für große kommerzielle Unternehmen) die Fähigkeit, die Verantwortung der Virusprüfung auf eine große Basis an Nutzern zu verteilen, die Menge an Informationen zum Virusstatus, die erzeugt und in einer Virusdatenbank zusammengefasst werden können, beträchtlich. Weiterhin die Nutzung eines Virusprüfers auf einem Computer einer dritten Partei, um grundsätzlich "Selbstprüfung" und "Selbstbestätigung" von Dateien, die von einer dritten Partei verwaltet werden, auszuführen. Darüber hinaus vergrößert das Bereitstellen der Fähigkeit, zusätzliche URLs an den Computer der dritten Partei zu senden, um zusätzliches Virusprüfen auszuführen, weiter die Arbeitsbasis, von der Informationen zum Virusstatus erzeugt werden können.

[0115] Andere Modifikationen werden für einen Fachmann ersichtlich sein. Deshalb umfasst die Erfindung die anschließend angefügten Ansprüche.

Patentansprüche

1. Verfahren, auf einem Computer ausgeführt, zur Bearbeitung einer Suchanfrage, wobei das Verfahren umfasst:

(a) Zugriff auf eine Computerdatenbank als Antwort auf eine Suchanfrage, um eine Ergebnismenge zu erzeugen, wobei die Ergebnismenge eine Vielzahl von Ergebnisdatensätzen identifiziert;

(b) Zugriff auf Informationen zum Virusstatus, die wenigstens einem Teil der Vielzahl der Ergebnisdatensätze zugeordnet sind; und

(c) Erzeugung einer Anzeigedarstellung von wenigstens einem Teil der Ergebnismenge auf der Grundlage der Informationen zum Virusstatus.

2. Verfahren nach Anspruch 1, wobei die Computerdatenbank wenigstens einen Webseitenindex und wenigstens ein Webseitenverzeichnis enthält, das eine Vielzahl von Datenbank-Datensätzen enthält, von denen jeder einen Uniform Resource Locator (URL) einer zugeordneten Computerdatei identifiziert.

3. Verfahren nach Anspruch 1, wobei die Erzeugung der Anzeigedarstellung die Erzeugung von Anzeigeinformationen, die einem ausgewählten Ergebnisdatensatz aus der Ergebnismenge zugeordnet sind, in der Anzeigedarstellung nur dann beinhaltet, falls die Informationen zum Virusstatus, die dem ausgewählten Ergebnisdatensatz zugeordnet sind, anzeigen, dass dem ausgewählten Ergebnisdatensatz ein geringes Risiko einer Infektion durch einen Computervirus zugetraut wird.

4. Verfahren nach Anspruch 1, wobei die Erzeugung der Anzeigedarstellung die Hervorhebung der Anzeigeinformationen beinhaltet, die einem aus der Ergebnismenge in der Anzeigedarstellung ausgewählten Ergebnisdatensatz zugeordnet sind, falls die Informationen zum Virusstatus, die dem ausgewählten Ergebnisdatensatz zugeordnet sind, anzeigen, dass dem ausgewählten Ergebnisdatensatz ein geringes Risiko einer Infektion durch einen Computervirus zugetraut wird.

5. Verfahren nach Anspruch 4, wobei das Hervorheben der dem ausgewählten Ergebnisdatensatz zugeordneten Anzeigeinformationen die Anzeige eines Icon nahe bei den Anzeigeinformationen beinhaltet, um anzuzeigen, dass dem ausgewählten Ergebnisdatensatz ein geringes Risiko einer Infektion durch einen Computervirus zugetraut wird.

6. Verfahren nach Anspruch 1, wobei die Erzeugung der Anzeigedarstellung das Hervorheben von Anzeigeinformationen beinhaltet, die einem ausgewählten Ergebnisdatensatz aus der Ergebnismenge in der Anzeigedarstellung zugeordnet sind, falls die Informationen zum Virusstatus, die dem ausgewählten Ergebnisdatensatz zugeordnet sind, anzeigen, dass dem ausgewählten Ergebnisdatensatz ein geringes Risiko einer Infektion durch einen Computervirus nicht zugetraut wird.

7. Verfahren nach Anspruch 6, wobei das Hervorheben der dem ausgewählten Ergebnisdatensatz zugeordneten Anzeigeinformationen das Anzeigen eines Icons nahe den Anzeigeinformationen beinhaltet, um anzuzeigen, dass dem gewählten Ergebnisdatensatz ein geringes Risiko einer Infektion durch einen Computervirus nicht zugetraut wird.

8. Verfahren nach Anspruch 6, das außerdem das Anzeigen von wenigstens einem Teil der Informationen zum Virusstatus enthält, die dem gewählten Ergebnisdatensatz als Antwort auf eine Nutzereingabe zugeordnet sind.

9. Verfahren nach Anspruch 8, wobei das Anzeigen der Informationen zum Virusstatus das Anzeigen der Informationen zum Virusstatus in einem aufklappenden Fenster beinhaltet, als Antwort auf eine Nutzereingabe, die auf ein nahe den Anzeigeinformationen angezeigtes Icon gerichtet ist.

10. Verfahren nach Anspruch 8, wobei das Anzeigen der Informationen zum Virusstatus das Anzeigen von wenigstens einem Namen einer infizierten Datei und einem Zeitstempel beinhaltet, der anzeigt, wann der ausgewählte Ergebnisdatensatz zuletzt auf Viren geprüft wurde.

11. Verfahren nach Anspruch 1, das weiterhin die Bestimmung umfasst, ob einem ausgewählten Ergebnisdatensatz aus der Ergebnismenge ein geringes Risiko einer Infektion durch einen Computervirus zugetraut wird, indem Informationen zum Virusstatus, die dem ausgewählten Ergebnisdatensatz zugeordnet sind, mit einem Viruskriterium verglichen werden.

12. Verfahren nach Anspruch 1, wobei das Viruskriterium wenigstens eines aus dem Folgenden bestimmt: ob ein Ergebnisdatensatz jemals mit einem Computervirus infiziert gefunden wurde, ob ein Ergebnisdatensatz innerhalb eines ersten vorher festgelegten Zeitraumes mit einem Computervirus infiziert gefunden wurde und ob ein Ergebnisdatensatz innerhalb eines zweiten, vorher festgelegten Zeitraumes auf Viren geprüft worden ist.

13. Verfahren nach Anspruch 1, das weiterhin beinhaltet:

(a) das Ausführen einer Virusprüfung für wenigstens einen Teil der Datensätze in der Computerdatenbank, um ihnen zugeordnete Informationen zum Virusstatus zu erzeugen; und

(b) das Speichern der Informationen zum Virusstatus, die während der Prüfung auf Viren erzeugt wurden, in einer Virusdatenbank;

wobei der Zugriff auf die Informationen zum Virusstatus, die dem Teil der Vielzahl der Ergebnisdatensätze zugeordnet sind, den Zugriff auf die Virusdatenbank beinhaltet.

14. Verfahren nach Anspruch 13, wobei das Ausführen der Virusprüfung während einer Crawling-Operation durchgeführt wird, und das Verfahren weiterhin das Ausführen einer Virusprüfung für einen ausgewählten Datensatz in der Datenbank umfasst, als Antwort auf wenigstens eines aus dem Folgendem: eine Modifikation einer dem ausgewählten Datensatz zugeordneten Datei und dem Ablauf eines Zeitraumes, seitdem der gewählte Datensatz zuletzt auf Viren geprüft wurde.

15. Verfahren nach Anspruch 13, wobei das Ausführen der Virusprüfung das Ausführen einer Virusprüfung für einen gewählten Datensatz aus der Computerdatenbank beinhaltet, indem wenigstens eine dem gewählten Datensatz zugeordnete Datei auf Viren geprüft wird sowie jede virusverdächtige Datei, die mit der zugeordneten Datei verlinkt ist.

16. Verfahren nach Anspruch 13, wobei das Ausführen der Virusprüfung das Ausführen einer Virusprüfung für wenigstens einen Teil der Vielzahl von Ergebnisdatensätzen vor der Erzeugung der Ergebnismenge beinhaltet.

17. Verfahren nach Anspruch 13, wobei das Ausführen der Virusprüfung weiterhin das Ausführen der Virusprüfung in einer Vielzahl von Computern beinhaltet, und das Verfahren außerdem das Empfangen von Informationen zum Virusstatus von wenigstens einem Teil

der Vielzahl von Computern umfasst.

18. Verfahren nach Anspruch 17, wobei das Empfangen der Informationen zum Virusstatus weiterhin die Authentifizierung der empfangenen Informationen zum Virusstatus beinhaltet, bevor die empfangenen Informationen zum Virusstatus in der Virusdatenbank gespeichert werden.

19. Verfahren nach Anspruch 17, wobei das Ausführen der Virusprüfung in der Vielzahl von Computern das Ausführen der Virusprüfung in einem Client-Computer beinhaltet, und das Verfahren weiterhin umfasst:

(a) das Ausgeben einer Suchanfrage vom Client-Computer; und

(b) das Empfangen und Anzeigen der Anzeigedarstellung von einem Teil der Ergebnismenge unter Benutzung des Client-Computers.

20. Verfahren nach Anspruch 19, wobei das Ausführen der Virusprüfung die Ausführung der Virusprüfung an einer gewählten Datei im Client-Computer beinhaltet, als Antwort auf eine Nutzeranforderung, die gewählte Datei abzufragen.

21. Verfahren nach Anspruch 17, das weiterhin enthält:

(a) das Senden eines Speicherplatz-Identifikators an einen aus der Vielzahl von Computern ausgewählten Computer;

(b) das Ausführen der Virusprüfung an einer ausgewählten Datei, die durch den Speicherplatz-Identifikator identifiziert wurde, um Informationen zum Virusstatus für die gewählte Datei zu erzeugen; und

(c) das Senden der der ausgewählten Datei zugeordneten Informationen zum Virusstatus vom ausgewählten Computer zur Aufnahme in die Virusdatenbank.

22. Verfahren nach Anspruch 17, wobei das Ausführen der Virusprüfung in der Vielzahl von Computern das Ausführen der Virusprüfung in einem ausgewählten Computer umfasst, indem eine Vielzahl von Dateien, auf die durch den ausgewählten Computer zugegriffen werden kann, virusgeprüft wird.

23. System, das enthält:

(a) eine Computerdatenbank, die eine Vielzahl von Datensätzen enthält; und

(b) ein Programm, das konfiguriert ist, um auf die Computerdatenbank als Antwort auf eine Suchanfrage zuzugreifen, um eine Ergebnismenge zu erzeugen, wobei die Ergebnismenge eine Vielzahl von Ergebnisdatensätzen aus der Vielzahl der Datensätze identifiziert, und das Programm weiterhin konfiguriert ist, um auf Informationen zum Virusstatus zuzugreifen, die wenigstens einem Teil der Vielzahl der Ergebnisdatensätze zugeordnet sind und auf der Grundlage der Informationen zum Virusstatus eine Anzeigedarstellung von wenigstens einem Teil der Ergebnismenge zu erzeugen.

24. System nach Anspruch 23, wobei die Computerdatenbank wenigstens einen Webseitenindex und ein Webseitenverzeichnis beinhaltet und wobei jeder Datensatz einen Uniform Resource Locator (URL) einer zugeordneten Computerdatei identifiziert.

25. System nach Anspruch 23, wobei das Programm konfiguriert ist, um die Anzeigedarstellung zu erzeugen, indem Anzeigeinformationen, die einem ausgewählten Ergebnisdatensatz aus der Ergebnismenge zugeordnet sind, in der Anzeigedarstellung nur erzeugt werden, falls Informationen zum Virusstatus, die dem ausgewählten Ergebnisdatensatz zugeordnet sind, anzeigen, dass dem ausgewählten Ergebnisdatensatz ein geringes Risiko einer Infektion durch einen Computervirus zugetraut wird.

26. System nach Anspruch 23, wobei das Programm konfiguriert ist, um die Anzeigedarstellung durch Hervorhebung der einem ausgewählten Ergebnisdatensatz aus der Ergebnismenge zugeordneten Anzeigeinformationen in der Anzeigedarstellung zu erzeugen, falls Informationen zum Virusstatus, die dem gewählten Ergebnisdatensatz zugeordnet sind, anzeigen, dass dem gewählten Ergebnisdatensatz ein geringes Risiko einer Infektion durch einen Computervirus zugetraut wird.

27. System nach Anspruch 23, wobei das Programm konfiguriert ist, um die Anzeigedarstellung durch Hervorhebung der einem ausgewählten Ergebnisdatensatz aus der Ergebnismenge zugeordneten Anzeigeinformationen in der Anzeigedarstellung zu erzeugen, falls Informationen zum Virusstatus, die dem ausgewählten Ergebnisdatensatz zugeordnet sind, anzeigen, dass dem ausgewählten Ergebnisdatensatz ein geringes Risiko einer Infektion durch einen Computervirus nicht zugetraut wird.

28. System nach Anspruch 23, wobei das Programm außerdem konfiguriert ist für die Bestimmung, ob einem ausgewählten Ergebnisdatensatz aus der Ergebnismenge ein geringes Infektionsrisiko durch einen Computervirus zugetraut werden kann, indem Informationen zum Virusstatus, die dem gewählten Ergebnisdatensatz zugeordnet sind, mit einem Viruskriterium verglichen werden.

29. System nach Anspruch 28, wobei das Viruskriterium wenigstens eines aus dem Folgenden bestimmt: ob ein Ergebnisdatensatz jemals durch einen Computervirus infiziert gefunden wurde, ob ein Ergebnisdatensatz innerhalb eines ersten, vorher festgelegten Zeitraumes durch einen Computervirus infiziert gefunden wurde und ob ein Ergebnisdatensatz innerhalb eines zweiten vorher festgelegten Zeitraumes auf Viren geprüft worden ist.

30. System nach Anspruch 23, das außerdem ein Crawler-Computerprogramm beinhaltet, das konfiguriert ist, um eine Virusprüfung für eine Vielzahl von Datensätzen aus der Computerdatenbank während einer Crawling-Operation auszuführen, und wobei das Crawler-Computerprogramm konfiguriert ist, die Virusprüfung für einen ausgewählten Datensatz in einer Computerdatenbank auszuführen, als Antwort auf wenigstens eines aus dem Folgenden: eine Modifikation einer dem gewählten Datensatz zugeordneten Datei und den Ablauf eines Zeitraumes, seit der gewählte Datensatz zuletzt auf Viren geprüft wurde.

31. System nach Anspruch 23, das weiterhin eine Virusdatenbank umfasst, die konfiguriert ist, um Informationen zum Virusstatus zu speichern, wobei das Programm konfiguriert ist, auf Informationen zum Virusstatus zuzugreifen, indem auf die Virusdatenbank zugegriffen wird, und wobei wenigstens ein Teil der Informationen zum Virusstatus vor der Erzeugung der Ergebnismenge in der Virusdatenbank vorhanden ist.

32. System nach Anspruch 31, wobei das Programm in einem ersten Computer vorhanden ist, der erste Computer außerdem konfiguriert ist, Informationen zum Virusstatus von einem zweiten Computer zu empfangen.

33. System nach Anspruch 32, wobei der zweite Computer in einer Vielzahl von Computern in Verbindung mit dem ersten Computer steht, wobei wenigstens ein Teil der Vielzahl von Computern konfiguriert ist, um die Virusprüfung und das Senden von Informationen

zum Virusstatus, die als Antwort auf das Virusprüfen erzeugt werden, auszuführen.

34. System nach Anspruch 33, wobei das Programm außerdem konfiguriert ist, um erhaltene Informationen zum Virusstatus vor dem Speichern der empfangenen Informationen zum Virusstatus in der Virusdatenbank zu authentifizieren.

35. System nach Anspruch 23, wobei der zweite Computer weiterhin konfiguriert ist, um die Suchanfrage auszugeben und für einen Teil der Ergebnismenge die Anzeigedarstellung zu empfangen und anzuzeigen.

36. System nach Anspruch 35, wobei einer aus der Vielzahl von Computern konfiguriert ist, die Virusprüfung einer gewählten Datei als Antwort auf eine Nutzeranforderung, die gewählte Datei abzufragen, auszuführen.

37. System nach Anspruch 23, wobei das Programm außerdem konfiguriert ist, um einen Speicherplatzidentifikator an einen aus der Vielzahl von Computern ausgewählten Computer zu senden, und wobei der ausgewählte Computer konfiguriert ist, um die Virusprüfung einer durch den Speicherplatzidentifikator bestimmten Datei auszuführen, um Informationen zum Virusstatus für die ausgewählte Datei zu erzeugen und die Informationen zum Virusstatus, die der gewählten Datei aus dem ausgewählten Computer zugeordnet sind, zur Aufnahme in die Virusdatenbank zu versenden.

38. System nach Anspruch 23, wobei die Ausführung der Virusprüfung in der Vielzahl von Computern die Ausführung der Virusprüfung in einem ausgewählten Computer beinhaltet, indem eine Vielzahl von Dateien, die für den ausgewählten Computer zugänglich sind, auf Viren geprüft werden.

39. Programmprodukt, das beinhaltet:

(a) ein Programm, das konfiguriert ist, um auf eine Computerdatenbank zuzugreifen, um als Antwort auf eine Suchanfrage eine Ergebnismenge zu erzeugen, wobei die Ergebnismenge eine Vielzahl von Ergebnisdatensätzen aus der Computerdatenbank identifiziert, und das Programm außerdem konfiguriert ist, um auf Informationen zum Virusstatus, die wenigstens einem Teil der Ergebnisdatensätze zugeordnet sind, zuzugreifen und auf der Grundlage von Informationen zum Virusstatus eine Anzeigedarstellung von wenigstens einem Teil der Ergebnismenge zu erzeugen; und

(b) ein signaltragendes Medium, dass das Programm trägt.

40. Programmprodukt nach Anspruch 39, wobei das signaltragende Medium wenigstens eines aus dem Folgenden beinhaltet: ein Aufnahmemedium und ein Übertragungsmedium.

41. Verfahren, auf einem Computer ausgeführt, zum Aufbau einer Virusdatenbank, wobei das Verfahren umfaßt:

(a) das Empfangen von Informationen zum Virusstatus, die von einer Vielzahl von Computern erzeugt wurden, mit einem ersten Computer, wobei die Informationen zum Virusstatus, die von jedem aus der Vielzahl von Computern, die wenigstens einer Datei zugeordnet sind, für den entsprechenden Computer aus der Vielzahl von Computern zugänglich ist; und

(b) das Speichern der Informationen zum Virusstatus für jede Datei in einer Virusdatenbank, die für den ersten Computer zugänglich ist.

42. Verfahren nach Anspruch 41, das weiterhin umfasst:

(a) das Zugreifen auf eine zweite Computerdatenbank als Antwort auf eine Suchanfrage, um eine Ergebnismenge zu erzeugen, wobei die Ergebnismenge eine Menge von Ergebnisdatensätzen identifiziert;

(b) das Zugreifen auf die Virusdatenbank, um Informationen zum Virusstatus abzufragen, die wenigstens einem Teil der Vielzahl der Ergebnisdatensätze zugeordnet sind; und

(c) das Erzeugen einer Anzeigedarstellung auf der Grundlage von Informationen zum Virusstatus von wenigstens einem Teil der Ergebnismenge.

43. Verfahren nach Anspruch 41, das weiterhin, während einer vom ersten Computer ausgeführten Crawling-Operation, die Ausführung der Virusprüfung einer Vielzahl von Dateien mit dem ersten Computer umfasst.

44. Verfahren nach Anspruch 41, das weiterhin die Authentifizierung von empfangenen Informationen zum Virusstatus vor der Speicherung der empfangenen Informationen zum Virusstatus in der Virusdatenbank umfasst.

45. Verfahren nach Anspruch 41, das weiterhin die Ausführung der Virusprüfung in einem Clientcomputer aus der Vielzahl von Computern umfasst, der konfiguriert ist, um eine Suchanfrage auszugeben und eine Anzeigedarstellung einer als Antwort auf die Suchanfrage generierten Ergebnismenge zu empfangen und anzuzeigen.

46. Verfahren nach Anspruch 45, wobei die Ausführung der Virusprüfung die Ausführung der Virusprüfung an einer ausgewählten Datei in dem Clientcomputer als Antwort auf eine Nutzeranforderung, die ausgewählte Datei abzufragen, beinhaltet.

47. Verfahren nach Anspruch 41, das weiterhin beinhaltet:

(a) das Senden eines Speicherplatz-Identifikators an einen aus der Vielzahl von Computern ausgewählten Computer;

(b) das Ausführen der Virusprüfung an einer ausgewählten Datei, die durch den Speicherplatz-Identifikator identifiziert wird, um Informationen zum Virusstatus für die gewählte Datei zu erzeugen; und

(c) das Senden der Informationen zum Virusstatus, die der ausgewählten Datei zugeordnet sind, vom gewählten Computer zur Aufnahme in die Virusdatenbank.

48. Verfahren nach Anspruch 41, wobei die Ausführung der Virusprüfung in der Vielzahl von Computern das Ausführen der Virusprüfung in einem aus der Vielzahl von Computern ausgewählten Computer beinhaltet, indem eine Vielzahl von Dateien, auf die durch den ausgewählten Computer zugegriffen werden kann, auf Viren geprüft werden.

49. System, das umfasst:

(a) eine Virusdatenbank, die konfiguriert ist, um Informationen zum Virusstatus für eine Vielzahl von Dateien zu speichern; und

(b) einen ersten Computer, in dem ein Programm vorhanden ist, das konfiguriert ist, um Informationen zum Virusstatus, die durch eine Vielzahl von Computern erzeugt werden, zu empfangen, wobei die Informationen zum Virusstatus, die von jedem aus der Vielzahl von Computern, die wenigstens einer Datei zugeordnet sind, für den jeweiligen Computer aus der Vielzahl von Computern zu-

gänglich sind, und das Programm weiterhin konfiguriert ist, um die Informationen zum Virusstatus für jede Datei in der Virusdatenbank zu speichern.

50. System nach Anspruch 49, das außerdem eine Vielzahl von Computern in Verbindung mit dem ersten Computer beinhaltet, wobei wenigstens ein Teil der Vielzahl von Computern konfiguriert ist, um Virusprüfungen auszuführen und Informationen zum Virusstatus, die als Antwort auf die Virusprüfung erzeugt wurden, zu versenden.

51. System nach Anspruch 49, wobei das Programm weiterhin konfiguriert ist, um empfangene Informationen zum Virusstatus zu authentifizieren, bevor die empfangenen Informationen zum Virusstatus in der Virusdatenbank gespeichert werden.

52. System nach Anspruch 50, wobei die Vielzahl von Computern einen Clientcomputer beinhaltet, der konfiguriert ist, um eine Suchanfrage auszugeben und eine Anzeigedarstellung von einem Teil der Ergebnismenge, die als Antwort auf die Suchanfrage erzeugt wurde, zu empfangen und anzuzeigen.

53. System nach Anspruch 50, wobei das Programm außerdem konfiguriert ist, um einen Speicherplatz-Identifikator an einen ausgewählten Computer aus der Vielzahl von Computern zu schicken, und wobei der ausgewählte Computer konfiguriert ist, um eine Virusprüfung an einer ausgewählten Datei, die durch den Speicherplatz-Identifikator bestimmt wird, auszuführen, um Informationen zum Virusstatus für die gewählte Datei zu erzeugen und die Informationen zum Virusstatus, die der ausgewählten Datei aus dem ausgewählten Computer zugeordnet sind, zur Aufnahme in die Virusdatenbank zu versenden.

54. Programmprodukt, das enthält:

(a) ein Programm, das sich in einem ersten Computer befindet und konfiguriert ist, um Informationen zum Virusstatus, die von einer Vielzahl von Computern erzeugt werden, zu empfangen, wobei die Informationen zum Virusstatus, die von jedem aus der Vielzahl von Computern generiert werden, wenigstens einer Datei, auf die von dem entsprechenden Computer aus der Vielzahl von Computern zugegriffen werden kann, zugeordnet sind, und das Programm weiterhin konfiguriert ist, um Informationen zum Virusstatus für die Datei in einer Virusdatenbank, die für den ersten Computer zugänglich ist, zu speichern; und

(b) ein signaltragendes Medium, dass das Programm trägt,

Hierzu 4 Seite(n) Zeichnungen

Nummer: DE 101 26 752 A1
Int. Cl.[7]: G 06 F 17/30
Offenlegungstag: 20. Dezember 2001

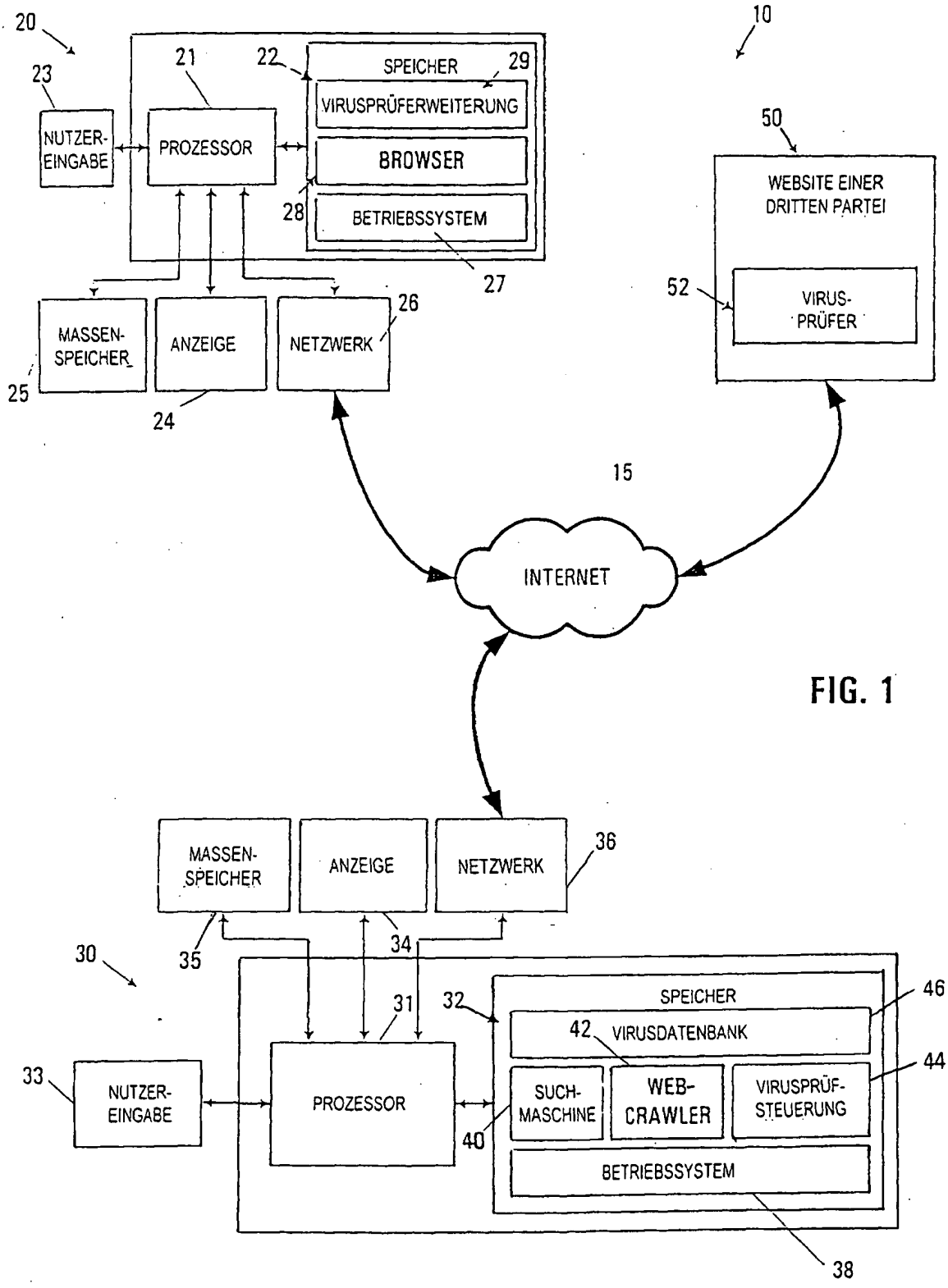


FIG. 1

101 510/740

Nummer: DE 101 26 752 A1
Int. Cl.[7]: G 06 F 17/30
Offenlegungstag: 20. Dezember 2001

FIG. 2

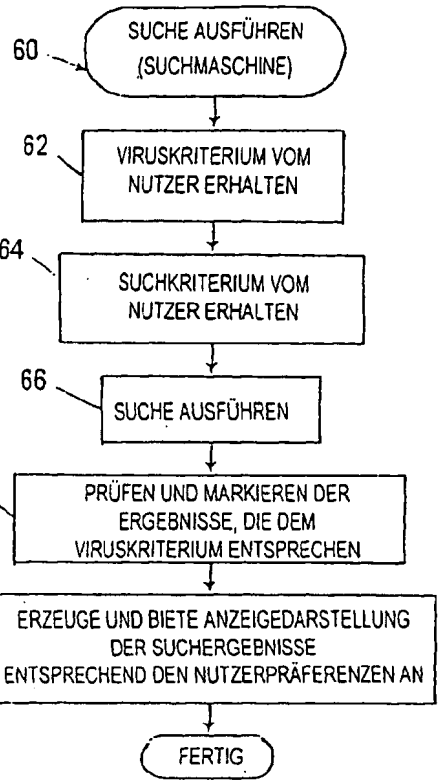
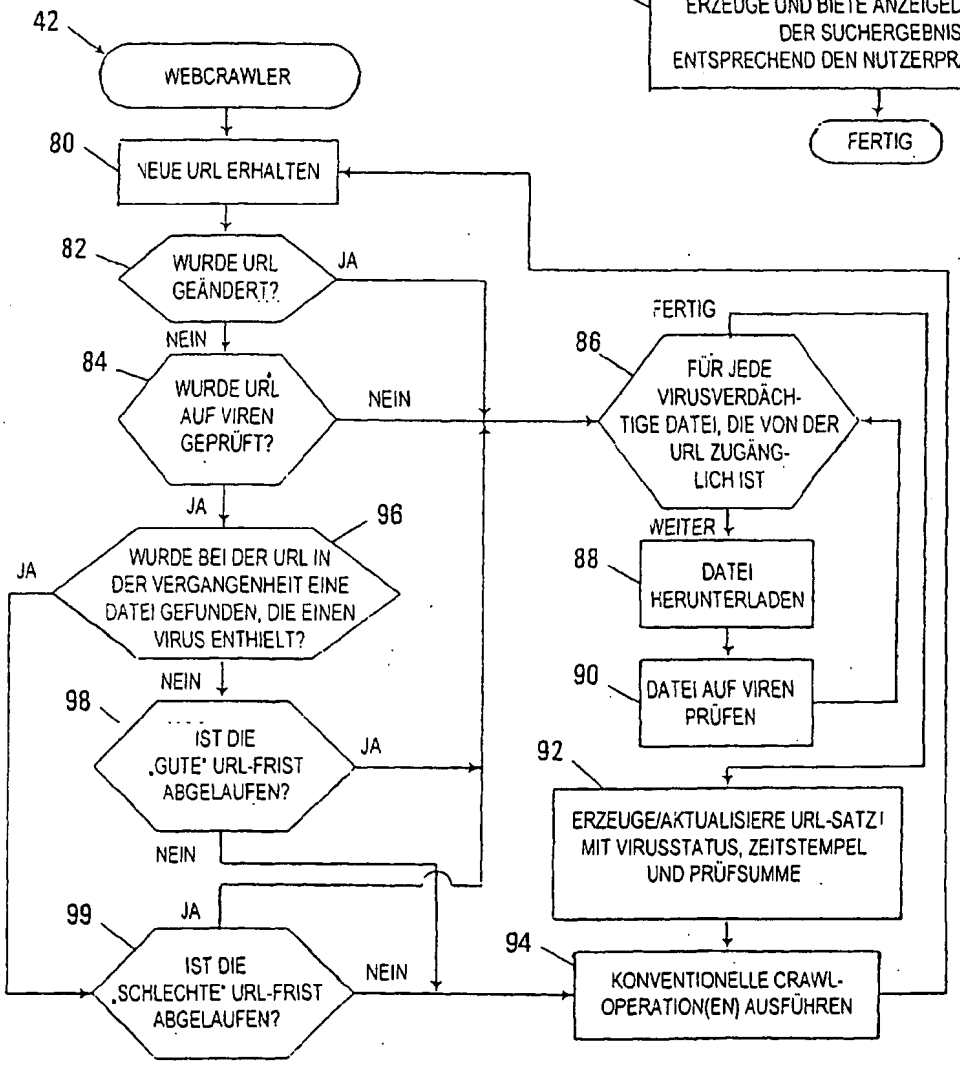


FIG. 3



101 510/740

Nummer: DE 101 26 752 A1
Int. Cl.[7]: G 06 F 17/30
Offenlegungstag: 20. Dezember 2001

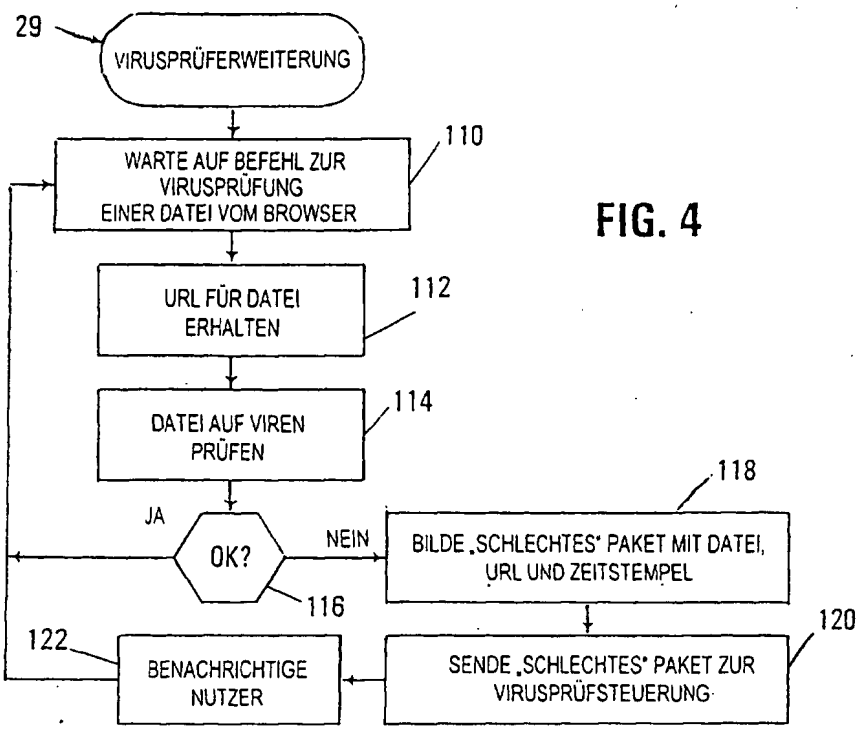


FIG. 4

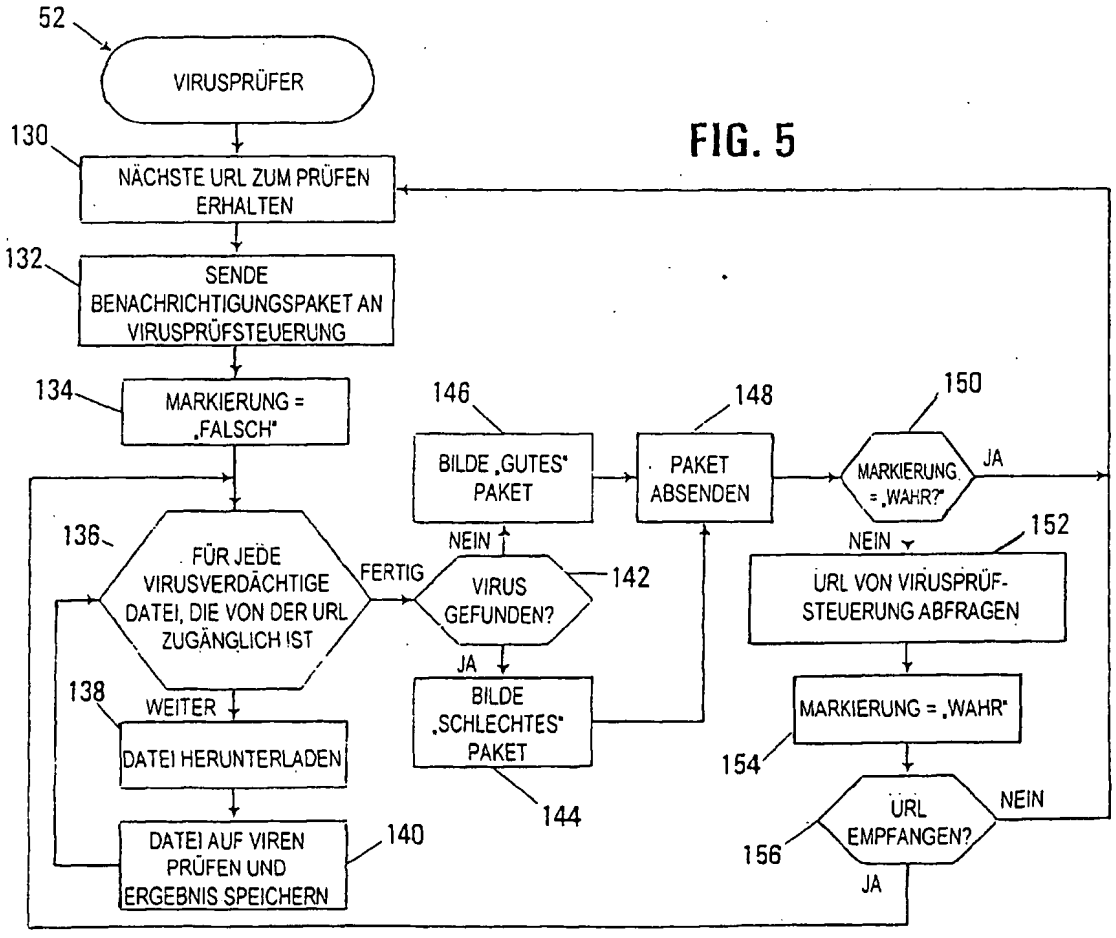


FIG. 5

101 510/740

Nummer: DE 101 26 752 A1
Int. Cl.[7]: G 06 F 17/30
Offenlegungstag: 20. Dezember 2001

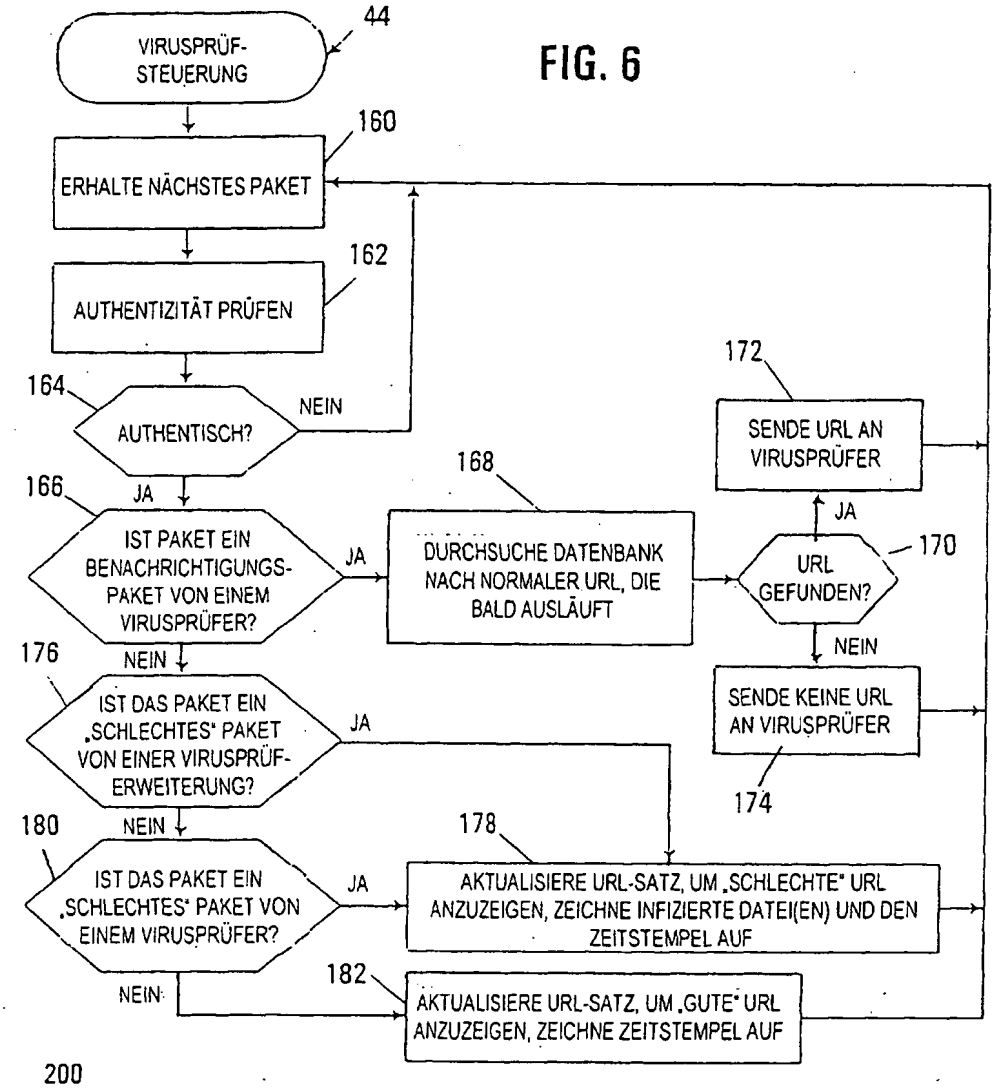


FIG. 6

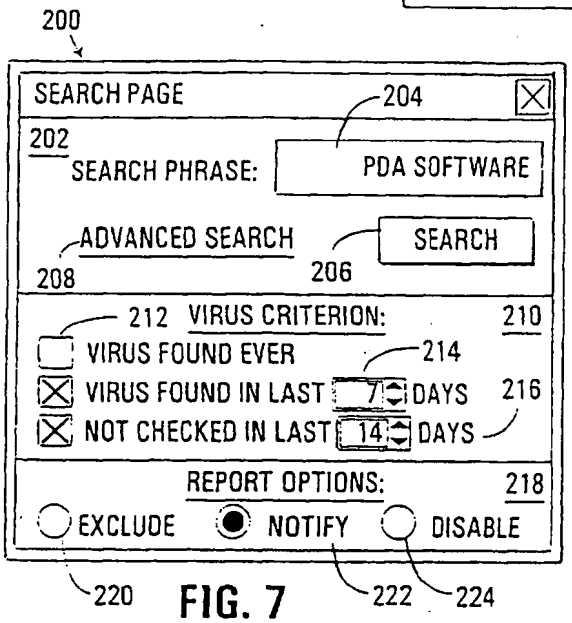


FIG. 7

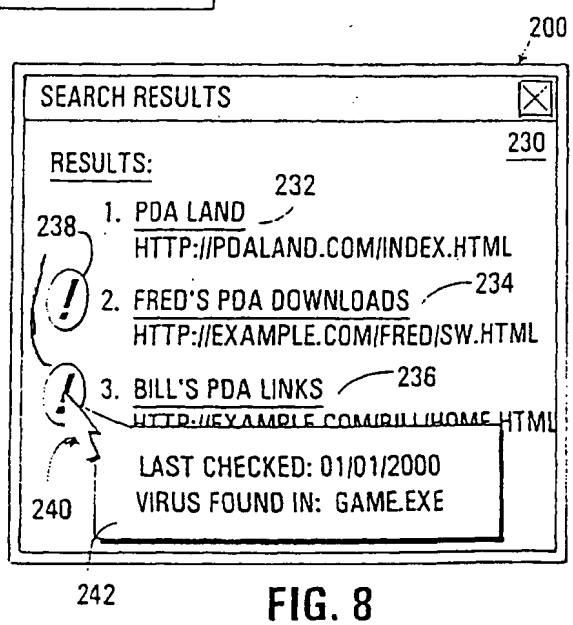


FIG. 8

101 510/740